UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

FEDERAL TRADE COMMISSION	)	
	)	
Plaintiff,	)	Hon. Richard D. Bennett
	)	
v.	)	Civil No.: RDB 08-CV-3233
	)	
INNOVATIVE MARKETING, INC., *et al.*	)	
	)	
Defendants.	)	

DEFENDANT KRISTY ROSS'S RESPONSE TO THE FTC'S STATEMENT OF MATERIAL FACTS

Dan K. Webb, *pro hac vice*
Thomas L. Kirsch II, *pro hac vice*
Winston & Strawn LLP
35 West Wacker Drive
Chicago, Illinois 60601
(312) 558-5600
dwebb@winston.com
tkirsch@winston.com

Carolyn Gurland, *pro hac vice*
2731 N Mildred Ave
Chicago, IL 60614
Phone: 312.420.9263
cgurland@comcast.net

RESPONSE TO THE FTC'S STATEMENT OF FACTS[1]

1. The Commission is an independent agency of the United States Government created by statute. 15 U.S.C. § 41 *et seq.*

2. The Commission is authorized to initiate court proceedings to enjoin violations of the Federal Trade Commission Act ("FTC Act"), and to secure such equitable relief as may be appropriate in each case, including restitution and disgorgement. 15 U.S.C. § 53(b).

3. This Court has jurisdiction over this matter pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

4. Venue in this district is proper under 28 U.S.C. §§ 1391(b) and (c) and 15 U.S.C. § 53(b). D.E. #3 (Ex. 20), Drexler Decl., p. 39, ¶114.

5. The activities of each of the Defendants, including the acts and practices set forth in the Complaint, are in or affecting commerce as defined in the FTC Act, 15 U.S.C. § 44. *See* MF ("MF") MF ##16, 35, 53. 54, 65-68, 70.

6. Kristy Ross was Vice President of Business Development for Innovative Marketing, Inc. ("IMI") commencing in 2006. Ross Affid., Vol I, Ex. 2, p. 7, ¶1; MF # 349.

7. Kristy Ross worked continuously for IMI from its inception in 2002 performing the same functions as Vice President but without a formal title. Ross Affid., Vol I, Ex. 2, p. 7, ¶1.

8. From approximately 2004-2007, Kristy Ross also assumed the duties of Chief Operating Officer and Chief Technology Officer of IMI after co-defendant Daniel Sundin fell ill. Sundin Affid., Vol. VIII, Ex. 89, p. 456, ¶15.

RESPONSE: MF # 8 is not accurate and misstates the Sundin Affidavit. The FTC claims that "from approximately 2004-2007, Kristy Ross also assumed the duties of Chief Operating Officer and Chief Technology Officer of IMI after co-defendant Daniel Sundin fell ill." (D.E. #186-3, Sundin Affid., Vol. VIII, Ex. 89, p. 456, ¶15 ("Sundin Affid.").) In fact, the portion of the Sundin affidavit cited by the FTC actually states that "from time to time, over the

[1]The FTC's MFs shall be referred to herein as "MF # ___." The Exhibits attached to this document shall be referred to as "RDX __." Contemporaneously with the filing of this document, Ms. Ross submits a Statement of Additional Facts. The Exhibits attached to Ms. Ross' Statement of Additional Facts shall be referred to as "DX __."

past three years" Sundin's illness affected his ability to devote time to his business endeavors, that during that time he had not "always been able to be actively engaged in" his IMI duties, and that "accordingly, some of [his] duties have been assumed from time-to-time" by Ms. Ross. (Sundin Affid., Vol. VIII, Ex. 89, p. 456, ¶15.)

> 9. Kristy Ross primarily focused on business expansion, sales and marketing, and product optimization while working for IMI. Ross Affid., Vol I, Ex. 2, p. 7, ¶1.
>
> 10. Kristy Ross managed large advertising accounts, approved IMI's deceptive advertisements for its computer security products, approved company expenditures, and led IMI's company-wide reorganization project. #mc, Vol. VII, Ex. 73, pp. 326, 335; #launch, Vol. VII, Ex. 74, p. 348, 350-354; network #co, Vol. VII, Ex. 75, pp. 363-369; Ex. C. to Sundin Affid., Vol. IX, Ex. 90, P. 59; Ex. I to D'Souza Affid., Vol. X, Ex. 97, pp. 222-256.

RESPONSE: MF #10 is not accurate. There is no evidence in the case that Kristy Ross managed any advertising account other than that with the AdOn/MyGeek network. There is no evidence that Kristy Ross approved "deceptive ads" for IMI computer security products. The evidence is to the contrary. (D.E. #186-3, #launch, Vol.VII, Ex. 74, p. 348; *see also* Gieron Depo., RDX 1, pp. 21:19-25; 110:25; 111:1-20; 113:6-11; 126:22-24; 165:23-25; 166:1-8; 185:3-10; 186:6-25; 187:1-23; 193:11-25; 194:1-4; 196:18-25; 197:1-6; 198:12-13; 201:6-19; 202:13-20; 229:1-12; 234:25; 235:1-22; 245:5-11; 266:1-16; 271:15-18; 274:18-23; 275:5-7; 275:13-16; 277:21-25; 281:7-8; 281:14-21; 289:22-25; 290:1-6; 291:2, 17-21; 294:4-7; 295:3-7; 331:2-13; 337:8-10; 369:2-3; 370:5-9; 373:5-25; 374: 1-35; 375:1-12; 389:12-25; 392:1-15; 396:6-9, 17-20; 419:17-21; 430:16-23; *see also* KRG30, RDX 2, p. 4; KRG 18, RDX 3, p. 1; KRG26, RDX 4, p. 3; KRG27, RDX 5, p. 4.)

The evidence cited also does not support the assertion that Kristy Ross led IMI's reorganization project. The email referred to as Ex. C to Sundin Affid., Vol. IX, Ex 90, p. 59 is the second page of an email from Sam Jain which mentions Kristy Ross only to state that

"Broost and Kristy have been developing the operations plan and they can also offer valuable support in organizing the marketing plans." Next line is "Once the basic strategy, org chart, and rough draft has been finalized; it can go out to matador, shiva, mike, and invisible, Conrad and other managers – and ask them to add and contribute their department plans to this." (Ex I to D.E. #186-3, D'Souza Affid., Vol. X, Ex. 97, pp. 222-256 (D'Souza Affid.") is a chart of IMI expenditures.) One column is "approved by," and Ms. Ross' name does appear in this column but with less frequency than that of many other names.

11. Kristy Ross placed millions of dollars in deceptive advertising for Defendants' products, including WinFixer, ErrorProtector, WinAntivirus, DriveCleaner, ErrorSafe, and SystemDoctor. MF # 212; D.E. #3 (Ex. 20), Drexler Decl., p. 37-38, ¶111; Ex. 3 to Gieron Depo., Vol. VIII, Ex. 87, pp. 84-85; MF # 362; Novick Decl., Vol. XII, Ex. 103, pp.13-15, ¶4.

RESPONSE: MF #11 is incorrect in its assertion that the ads placed by Kristy Ross were "deceptive." Nothing in the listed evidence supports the assertion of deceptiveness. In fact, Mr. Gieron of MyGeek/AdOn testified that he approved Kristy Ross's ads, that he did not recall approving many of the ads complained about by MyGeek traffic partners, , and that some of Ms. Ross's ads were at most annoying, but not deceptive. (Gieron Depo., RDX 1, pp. 158:6-9; 245:5-11; 274:18-23; 275:5-7; 275:13-16; 281:7-8; 281:14-21; 287:19-22; 288:5-16; 289:22-25; 290:1-6, 291:2; 368:10-11; 368:21-22; 369:2-3; 370:5-9; 419:17-21; 430:16-23; *see also* KRG 18, RDX 3, p. 1; KRG 6, RDX 6, p. 3.)

12. IMI was incorporated in 2002 pursuant to the laws of Belize and headquartered in the Ukraine. Sundin Affid., Vol. VIII, Ex. 89, p. 453 ¶4, 454 ¶10.

13. IMI was also referred to by the defendants as Globedat, a name that was interchangeable with and used to mean Innovative Marketing, Inc. Ex. D to Sundin Affid., Vol. IX, Ex. 90, p. 60.

RESPONSE: MF #13 is not supported by Ex. D. to Sundin Affid., Vol. IX, Ex 90, p. 60. This is a one page letter from Marc D'Souza to Broost subject Marketing pdf dated 1/18/06

with a line "1. Globedat - > Innovative Marketing" evidently as a suggested change to the marketing pdf. This exhibit shows that Marc D'Souza referred to Globedat as Innovative Marketing in a letter not that "the defendants" used Globedat and Innovative Marketing interchangeably.

14. IMI was created by defendant Daniel Sundin to sell computer security software products, which were marketed through IMI-owned and maintained websites. Sundin Affid., Vol. VIII, Ex. 89, pp. 452-453, ¶3, 454 ¶9.

RESPONSE: MF #14 misstates the Sundin affidavit. The affidavit does not state that Sundin created IMI to "sell computer security software products" but that he created it "to organize a vast international team to develop and build products." (Sundin Affid., Vol. IX, Ex. 90, p. 60.)

15. The products sold by IMI include Winfixer, Winantivirus, Winantiviruspro, Winantispyware, Popupguard, Winfirewall, Internetantispy, Winpopupguard, Computershield, Winantispy, Pcsupercharger, Errorsafe, Sysprotect, Drivecleaner, Systemdoctor, and Errorprotector. Ex. E. to Sundin Affid., Vol. VIII, Ex. 89, pp. 467 - 470; Novick Decl., Ex. 103, Vol. XII, pp.13-15, ¶4.

16. The products listed in MF # 15 have generated more than 1,300 consumer complaints to the FTC. FTC consumer complaints, Vol. I-V, Ex. 54; Novick Decl., Vol. XII, Ex. 103, p.13-15, ¶4.

17. The products listed in MF # 15 are detected as system threats by every major computer security vendor. D.E. #3 (Ex. 20), Drexler Decl., pp. 8-11, ¶28-32.

RESPONSE: MF# 17 is not accurate and is not supported by the Drexler Declaration. Ms. Drexler's declaration actually states that McAfee identified some of products listed in MF #15 as "unsafe." (D.E. #3 (Ex. 20), Drexler Dec., ¶ 30 ("Drexler Dec.").) Ms. Drexler does not opine that McAfee identified the products as system threats, nor does Ms. Drexler opine that "every major computer security vendor" detected the products as system threats. (Drexler Dec., ¶¶ 28-32.) The FTC's implication that the products listed in MF #15 did not work is not supported by the record. Indeed, Scott Ellis, Ms. Ross's expert witness tested the paid version of

DriveCleaner and concluded as follows:

> DriveCleaner is a feature rich software that performs many of the same functions as comparable products, and does so successfully. DriveCleaner performs similarly to other system cleaners of the same time period and removed files as claimed. I detected no abnormal operation or suspicious behavior. DriveCleaner presented no issues or difficulties uninstalling from the test system at the completion of testing. Many major competitors including public companies such as Symantec and McAfee offer products with similar (and often less comprehensive) features than does DriveCleaner.

(Expert Report of Scott Ellis, RDX 7, p. 11.)

18. The sale of the products listed in MF # 15 was responsible for almost all of IMI's revenue. Sundin Affid., Vol. VIII, Ex. 89, p. 455, ¶12.

19. Sam Jain was an original founding partner of IMI in 2002 and was the Chief Executive Officer of IMI. Jain Affid., Vol. IX, Ex. 95, p. 327, ¶1, p. 328, ¶¶3-5.

20. Sam Jain was involved in all aspects of IMI's business affairs, including marketing and sales. Jain Affid., Vol. IX, Ex. 95, p. 328 ¶¶3-6, p. 332, ¶25.

21. Sam Jain personally invested a large amount of capital into IMI. Jain Affid., Vol. IX, Ex. 95, p. 328, ¶4.

22. Sam Jain developed relationships with payment processors to process IMI's credit card transactions and approved expenditures of IMI's resources. D.E. #3 (Ex. 17, Att. B) D'Souza Counterclaim, pp. 99-100, ¶109, 112; Jain Affid., Vol. IX, Ex. 95, p. 334, ¶32; Ex. I to D'Souza Affid., Vol. X, Ex. 97, pp. 222-256.

23. Daniel Sundin incorporated IMI in 2002. Sundin Affid., Vol. VIII, Ex. 89, p. 452, ¶1.

24. Daniel Sundin, Sam Jain and Kristy Ross collaborated together to start the IMI business venture. Sundin Affid., Vol. VIII, Ex. 89, p. 453, ¶6.

RESPONSE: MF #24 omits the fact that only Daniel Sundin and Sam Jain had the extensive discussions that led to Sundin's agreement to join the business venture and that ultimately, Sundin agreed to enter into an agreement with Jain in which Sundin and Jain would take the lead roles in the business venture. (Sundin Affid., Vol. VIII, Ex. 89, p. 453, ¶6.)

25. Daniel Sundin used IMI to develop computer security software products to offer to consumers. Sundin Affid., Vol. VIII, Ex. 89, pp. 454-455, ¶¶9-10.

26. Daniel Sundin held the positions of Chief Operating Officer and Chief Technology Officer of IMI from 2002. Sundin Affid., Vol. VIII, Ex. 89, p. 452, ¶1.

27. Daniel Sundin was chief designer of IMI's software security products. D.E. #3 (Ex. 17 Att. A), Claim, p. 57, ¶22.

28. Daniel Sundin commenced IMI's operations in Kiev, Ukraine in 2002 and the Ukraine facility became IMI's headquarters. Sundin Affid., Vol. VIII, Ex. 89, p. 455, ¶11.

29. Daniel Sundin was owner of Vantage Software. Sundin Affid., Vol. IX, Ex. 90, p. 5, ¶6.

30. Vantage Software was used to register virtually all of IMI's domains, including *innovativemarketing.com*, *winantivirus.com*, and *drivecleaner.com*. Tucows Records, Vol. VII, Ex. 68, pp. 205-247; MF # 347.

31. Daniel Sundin's credit card was used to pay for advertisements that Kristy Ross placed with the advertising network, MyGeek. Ex. 6 to Gieron Depo., Vol. VIII, Ex. 87, pp. 188-189.

RESPONSE: MF #31 is not established by Ex 6 to Gieron Depo., RDX 1, pp. 188-189 as this exhibit shows a credit card used pay MyGeek, but does not alone link that credit card to Daniel Sundin.

32. Despite valid service, Sundin chose not to appear to defend himself in this action. D.E. #87; D.E. # 161.

33. James Reno is a long time business associate of Sam Jain, and was sued along with Jain by Symantec Corporation in 2004 for pirating Symantec's software. D.E. #3 (Ex. 20), Drexler Decl., pp. 29-30, 35, ¶85, 102.

34. James Reno is the owner of Bytehosting Internet Services, LLC. D.E. #3 (Ex. 17, Att. B) D'Souza Counterclaim, p. 81, ¶50; Reno Decl., D.E. #69 (Ex. 3), ¶2.

35. James Reno used Bytehosting for support services for IMI including operating the customer support call center for IMI's computer security products. Junction Networks Records, Vol. VI, Ex. 55, pp. 2-15; MF # 348; Ex. C to D'Souza Affid., Vol. IX, Ex. 94, p. 271; Reno Decl., D.E. #69 (Ex. 3), ¶3.

36. James Reno purchased and maintained computer equipment for the IMI Enterprise. Ex. I to D'Souza Affid., Vol. X, Ex. 97, p. 228.

37. James Reno managed the content delivery contract with LimeLight Networks. Torrez Decl., Vol. VI, Ex. 56, p. 16, ¶4; MF # 365.

38. James Reno used the name setupahost as contact information for IMI business. Torrez Decl., Vol. VI, Ex. 56, p. 16, ¶¶3-4; #pro, Vol. VII, Ex. 77, p. 372; #comodo, Vol. VII, Ex. 78, pp. 373-375.

39. ByteHosting was referred to as IMI's "Ohio office." D.E. #3 (Ex. 17, Att. B) D'Souza Counterclaim, p. 81, ¶¶81-82, 108; Ex. C to D'Souza Affid., Vol. IX, Ex. 94, p. 271.

40. IMI wired funds to Bytehosting for the purpose of paying payroll, rent, taxes, and utilities. Ex. KK to D'Souza Affid., Vol. XI, Ex. 97, p. 37; Ex. A and I to Jain Affid., Vol. IX, Ex. 95, pp. 379-380, 384; Ex. C. to Jain Affid., Vol. X, Ex. 96, p. 22; D.E. #3 (Ex. 20), Drexler Decl., p. 329, ¶6.

41. Marc D'Souza joined IMI with defendants Sam Jain, Daniel Sundin, and Kristy Ross in 2002. Jain Affid., Vol. IX, Ex. 95, pp. 379-380, 384.

RESPONSE: MF #41 is not established by D.E. #186-3, Jain Affid., Vol. IX, Ex. 95, pp. 379-380, 384 ("Jain Affid.") The cited exhibits are lists of account numbers with wire transfer instructions and a profit and loss by month statement which do not relate to D'Souza joining IMI.

42. Although IMI did not use formal titles, Marc D'Souza functioned as a Managing Partner, Chief Financial Officer, and Chief Marketing Director of IMI. Ex. C to D'Souza Affid., Vol. IX, Ex. 94, p. 274; D'Souza Affid., Vol. IX, Ex. 93, p. 175, ¶17; Ex. E. to Sundin Affid., Vol. IX, Ex. 90, p. 66.

43. Marc D'Souza was responsible for developing relationships with payment processors that could process the huge volume of sales generated by IMI. D.E. #3 (Ex. 17, Att. B) Counterclaim, p. 105, ¶¶133 - 137.

44. Marc D'Souza owns Synergy Software, BV which controlled several of the merchant accounts used by the Defendants to bill consumers for their products. D.E. #3 (Ex. 17, Att. B), Counterclaim, p. 114, ¶178; D.E. #3 (Ex. 20), Drexler Decl., p. 42, ¶127.

45. IMI had great difficulty maintaining relationships with payment processors due to the high rate of chargebacks and complaints from defrauded consumers. D.E. #3 (Ex. 20), Drexler Decl., p. 41, ¶125; D.E. #3 (Ex. 17, Att. B) D'Souza Counterclaim, p. 89, ¶¶81-83.

RESPONSE: MF #45 cites to the Drexler Ex., which in turn cites to the D'Souza

Counterclaim. What the FTC fails to inform the Court, however, is that an October 23, 2007 Order of the Canadian Court, which is not referenced in the Drexler Ex. or Declaration and is not included in the 12 volumes of Summary Judgment Exhibits, struck the D'Souza Statement of Defence and Counterclaim, D'Souza Counterclaim, RDX 8, because it was an irregular and improper pleading and an abuse of this Honorable Court's process. The Court further fined D'Souza $30,000 for this false submission.

> 46. Marc D'Souza was one of the few people at IMI who could review and authorize payments of IMI's business expenses as well as review and approve advertising and marketing campaigns. D'Souza Affid., Vol. IX, Ex. 92, p. 133, ¶¶42-43, p. 140, ¶ 64; Ex. I to D'Souza Affid., Vol. X, Ex. 97, pp. 222-256; sysadmin, Vol. VII, Ex. 79, pp. 377-380, #mc, Vol. VII, Ex. 73, p. 321, 325, #sm, Vol. VII, Ex. 80, p. 382, 389, 391-93, 397, 399, 401.
>
> 47. Maurice D'Souza, Marc's father, was directly involved in setting up the various merchant accounts the IMI Defendants used to process consumer payments, and kept track of all of IMI's accounts. D'Souza Affid., Vol. IX, Ex. 92, p. 131, ¶¶34-35.
>
> 48. Maurice D'Souza had no contract or other compensation agreement with the IMI. D.E. #3 (Ex. 17, Att. C) Claim, p.10.
>
> 49. At least $18 million of IMI's assets resided at one time in Maurice's personal and corporate bank accounts. Jain Affid., Vol. IX, Ex. 95, p. 346, ¶67.
>
> 50. In 2007, Marc and Maurice D'Souza were sued by IMI in the Ontario Superior Court of Justice. The suit alleged that the D'Souzas embezzled money from IMI and were wrongfully withholding the profits of the business from defendants Jain, Sundin, and Ross. D.E. #3 (Ex. 17, Att. C) Claim, pp. 4-16.

RESPONSE: MF # 50 misstates the evidence in that it contends that the D'Souzas withheld profits of IMI from Kristy Ross. There is no evidence that Ms. Ross received any profits when the Canadian litigation was settled, even though Ms. Drexler's affidavit states that D'Souza embezzled $48 million and the FTC claims below in MF #51 that D'Souza kept $8.2 million (which therefore assumes that Mr. Jain and Mr. Sundin received some substantial amount back from D'Souza). Further, the evidence is clear that Ms. Ross was not a party to the

referenced Canadian litigation, which the FTC admits in MF # 221 below. Moreover, as Ms. Drexler, the FTC's investigator makes clear in her Declaration, Marc D'Souza's Counterclaim was against Jain and Sundin for damages for breach of fiduciary duty to the Business partnership. (Drexler Dec., ¶ 21.) Mr. D'Souza did not sue Ms. Ross for breach of fiduciary duty because Ms. Ross, as a mere employee, did not owe any fiduciary duties.

51. The suit was eventually resolved through a settlement that permitted the D'Souzas to keep more than $8.2 million of corporate profits. Settlement Agreement, Vol. XI, Ex. 98**,** p. 443.

52. The Defendants created advertisements that appeared to scan consumers' computers for errors and dangerous files and warn consumers that errors and other threats were detected on their computers. Ex. E to Sundin Affid., Vol. VIII, Ex. 89, p. 465; D.E. #3 (Ex.20), pp. 52-69; Ex. 9 to Webster Depo., Vol. 6, Ex. 57, pp. 126-139**;** MF # 361; #mc, Vol. VII, Ex. 73, p. 326, 341; #launch, Vol. VII, Ex. 74, pp. 346-347, 351, 352, #sm, Vol. VII, Ex. 80, pp. 385-388; *See, e.g.* Exs. 13-15, 20, and 23 to Gieron Depo., Vol. VIII, Ex. 87, pp. 246-251, 261, 264, 286, 318-319.

RESPONSE: MF #52 is not supported by the exhibits listed. *First*, the MF refers to "Defendants" without differentiation. None of the exhibits, however, establish that Kristy Ross "created" advertisements that appeared to scan customers' computers. Indeed, Mr. Gieron testified at his deposition that he had no information that Ms. Ross was responsible for the content of any of the ads. (Gieron Depo., RDX 1, pp. 196:18-25-197:1-6; 266:1-6; 266:7-16.) *Second*, there is no evidence Ms. Ross placed any ads with Valueclick, and at his deposition, the Valueclick representative confirmed that he had no information that Ms. Ross placed any advertising with his company. (Webster Depo., RDX 9, pp. 105:4-6; 105:17-23; 108:7-18.) *Third*, the exhibits listed from the Gieron deposition contain screen shots of certain ads Ms. Ross purportedly placed at MyGeek/AdOn, but do not establish that these were created by Kristy Ross. (Gieron Depo., RDX 1, pp. 196:18-25; 197:1-6; 266:1-6; 266:7-16.)

53. The Defendants disseminated the advertisements described in MF # 52 to consumers both in the United States and abroad primarily through advertising networks.

Ex. C to D'Souza Affid., Vol. IX, Ex. 94, p. 279.

RESPONSE: MF #53 does not establish that the ads in #52 were "disseminated primarily through advertising networks." The chart contained on this page is a pie chart of geographic sales by region and contains no information about advertising networks.

54. Two of the major Internet advertising networks the Defendants used to disseminate their advertisements were Valueclick/Mediaplex ("ValueClick") and AdOn Network (formerly known as MyGeek Network and hereinafter referred to as "MyGeek"). Gieron Depo., Vol. VIII, Ex. 87, p. 9 (31:4-19); Ex. 3 to Webster Depo., Vol. 6, Ex. 57, pp. 75-80.

RESPONSE: MF # 54 is inaccurate to the extent it refers to "Defendants" generally. The evidence is clear that Ms. Ross worked with AdOn / MyGeek but did not work with Valueclick. (Webster Depo., RDX 9, pp. 105:4-6; 105:17-23; 108:7-18.)

55. IMI disseminated its advertisements through ValueClick using the company name Revenue Response. Ex. 5 to Webster Depo., Vol. VI, Ex. 57, pp. 83, 84, 86, 89; Ex. 13 to Webster Depo., Vol. VI, Ex. 57, pp. 146-149.

RESPONSE: *See* Response to MF # 54 above.

56. Many of the Defendants' bogus advertisements appeared to be warnings directly from the Microsoft Windows operating system. Cucura Decl., Vol. I, Ex. 7, p. 16, ¶2; Dubois Decl., Vol. I, Ex. 9, p. 20, ¶3; Eykelhoff Decl., Vol. I, Ex. 10, p. 22, ¶2; Fieler Decl., Vol. 1, Ex. 12, p. 26, ¶3; Furney Decl., Vol. I, Ex. 15, p. 30, ¶3; Golden Decl., Vol. I, Ex. 16, p. 33, ¶2; Hodge Decl., Vol. I, Ex. 20, p. 41, ¶3; Kilthau Decl., Vol. I, Ex. 25, p. 50, ¶2; Layton Decl., Vol. I, Ex. 26, p. 52, ¶9; Levens Decl., Vol. I, Ex. 27, p. 54, ¶3; Lovell Decl., Vol. I, Ex. 29, p. 57, ¶4; Marcynzsyn Decl., Vol. I, Ex. 30, p. 59, ¶3; Martin Decl., Vol. I, Ex. 31, p. 62, ¶2; Randall Decl., Vol. I, Ex. 40, p. 76, ¶5; Richgels Decl., Vol. I, Ex. 42, p. 80, ¶2; Stalvey Decl., Vol. I, Ex. 46, p. 86, ¶2; Welander Decl., Vol. I, Ex. 50, p. 93, ¶2; White Decl., Vol. I, Ex. 51, p. 95, ¶2; Wirkman Decl., Vol. I, Ex. 52, p. 97, ¶3; D.E. #3 (Ex. 20), Drexler Decl., pp. 91-93, 96-100.

RESPONSE: MF #56 is inaccurate. MF # 56 refers to "Defendants' bogus ads" but fails to establish that even one of the ads complained about was placed by Kristy Ross. In addition, MF #56 depends on the affidavits of consumers who make different statements about why they reached the conclusions that the ads they saw appeared to be from the Microsoft

operating system. These untested conclusions do not establish which ads the consumers saw, or whether those ads did in fact appear to come from the Microsoft operating system or if that appearance rose to the level of deceptiveness.

57. In creating these ads, the Defendants misappropriated the "look and feel" of the Windows operating system, including the Windows Security Center, the trademarked Windows Security Shield logo, and the dialog boxes Windows uses to warn users of errors. Declaration of Microsoft Trademark Paralegal Jennifer Bollen, Vol. VI, Ex. 59, p. 171, ¶9; MF # 350; Ex. 9 to Webster Depo., Vol. 6, Ex. 57, pp. 126-139; #launch, Vol. VII, Ex. 74, pp. 346-347; Kim Depo., Vol. VII, Ex. 86, p. 469.

RESPONSE: MF #57 is inaccurate. MF# 57 states that in creating the ads in MF #56, "Defendants" misappropriated the 'look and feel' of the Windows operating system. . . ." There is no evidence that any of the complained about ads was created or placed by Kristy Ross. Indeed, in that the MF refers to the Value Click network ads, to the deposition of the ValueClick witness and to the section of Marc D'Souza's expert deposition in which he was questioned about ads placed on the ValueClick network, it suggests that the ads were not placed by Ms. Ross who was not established to have ever had any dealings with this advertising network. Moreover, the statement, on its face, contains a conclusion as to the "look and feel" of ads that cannot be established without the specific basis of the assertion being tested.

58. Hundreds of millions of these fake Windows alert ads ran on the ValueClick network. Ex. 9 to Webster Depo., Vol. 6, Ex. 57, pp. 126-139.

RESPONSE: *See* Response to MF # 54 above.

59. These ads displayed the yellow exclamation point and red "X" graphics that are identical to the graphics Microsoft Windows uses when it declares a real error to the user and falsely warned consumers that an error had occurred on their computer and encouraged them to click on the ad for a free scan. Ex. 3 to Webster Depo., Vol. VI, Ex. 57, p. 76; Kim Depo., Vol. VII, Ex. 86, p. 469.

RESPONSE: *See* Response to MF # 54 above.

60. These warning messages were static images. Expert Report of Kevin Johnson, Vol. VI, Ex. 63, p. 494.

61. The defendants created advertisements with elaborate animations that actually appeared to conduct a scan of consumers' computers. D.E. #3 (Ex. 20), Drexler Decl., p. 69, ¶205; Ex. D to Sundin Affid., Vol. VIII, Ex. 89, p. 465; #sm, Vol. VII, Ex. 80, pp. 385-388; #launch, Vol. VII, Ex. 74, p. 348; #mc, Vol. VII, Ex. 73, pp. 326, 337-338; Davis Decl., Vol. I, Ex. 8, p. 18, ¶2; Hunt Decl., Vol. I, Ex. 21, p. 43, ¶2; Hurd Decl., Vol. I, Ex. 22, p. 44, ¶3; Marcynzsyn Decl., Vol. I, Ex. 30, p. 59, ¶4; Oswald Decl., Vol. I, Ex. 35, p. 68, ¶3; Renteria Decl., Vol. I, Ex. 41, p. 78, ¶5, Woerner Decl., Vol. I, Ex. 53, pp. 99-101.

RESPONSE: MF #61 misconstrues the evidence. MF# 61 asserts that "defendants created advertisements . . . ." There is no evidence that defendant Ross ever created any ad, much less an ad that appeared to scan a computer. The facts are to the contrary. The MF fails to cite to the Gieron deposition and exhibits which actually contained examples of ads that may have resembled ads Ms. Ross placed with the MyGeek/AdOn network. The overwhelming majority of these ads have never even been alleged to have issues with fake scanning. (Gieron Depo., RDX 1, pp. 257:15-18; 258:21-25-259:1-4; 275:13-16; 289:22-25; 419:10-21; 421:6-8; 422:6-9; 445:20-24; 441:7-13.) With respect to the single ad alleged to have falsely claimed to scan a computer, the FTC's evidence is lacking in four respects. *First*, Gieron was uncertain about the functionality of the ad in question. (Gieron Depo., RDX 1, pp. 345:18-22; 349:14-17.) *Second*, the links tested by AdOn which appear to have resulted in a scan differ from the links that Ms. Ross sent to AdOn and the ads that launched at AdOn. (Gieron Depo., RDX 1, pp. 181:18-25; 182:1-3; 354:15-21; 356:23-25; 357:1.) *Third*, to the extent that Ms. Ross' comment about the screen shots from the AdOn test is relied upon to establish Ms. Ross' knowledge of the functionality of the ad, there is no evidence that Ms. Ross saw the precise same ad that AdOn saw based on possible differences in her computer and browser. (Gieron Depo., RDX 1, pp. 201:6-19; 202:13-20; *see also* KRG 27, RDX 5, p. 4.) *Fourth*, and most importantly, Gieron was unable to conclude that the ad with the scanner information was ever seen in the form shown in

the screen shots by any US consumer. (Gieron Depo., RDX 1, pp. 145:11-25; 146:1-2.)

62. At the conclusion of these fake scans, the defendants informed consumers that their computers were riddled with errors, dangerous files, and the like. D.E. #3 (Ex. 20), Drexler Decl., p. 69, ¶205; Ex. D to Sundin Affid., Vol. VIII, Ex. 89, p. 465; #launch, Vol. VII, Ex. 74, p. 348; #mc, Vol. VII, Ex. 73, p. 326; Davis Decl., Vol. I, Ex. 8, p. 18, ¶2; Hunt Decl., Vol. I, Ex. 21, p. 43, ¶2; Hurd Decl., Vol. I, Ex. 22, p. 44, ¶3; Marcynzsyn Decl., Vol. I, Ex. 30, p. 59, ¶4; Oswald Decl., Vol. I, Ex. 35, p. 68, ¶3; Renteria Decl., Vol. I, Ex. 41, p. 78, ¶5, Woerner Decl., Vol. I, Ex. 53, pp. 99-101.

RESPONSE: MF #62 misstates the evidence. MF #62 asserts that "defendants informed consumers. . . ." There is no evidence that defendant Kristy Ross "informed consumers" or created an ad that informed consumers that their computers were riddled with errors after a fake scan. The facts are to the contrary. (Gieron Depo., RDX 1, pp. 196:18-25; 197:1-6; 266:1-6; 266:7-16.) What the evidence actually establishes is that the overwhelming majority of the ads which were the subject of the Gieron deposition may have been annoying, but did not contain deceptive attributes or false statements and that the single ad that the FTC cites to support the assertion that Ms. Ross placed an ad with a scanning attribute suffers from major evidentiary problems. *See* Response to MF # 61 above.

63. The Defendants specifically designed these system scan advertisements to scare consumers into believing that they had errors, pornographic files, and dangerous files on their computers. #launch, Vol. VII, Ex. 74, pp. 346-347; #mc, Vol. VII, Ex. 73, p. 326.

RESPONSE: MF #63 states that "defendants specifically designed these system scan advertisements to scare consumers…" There is no evidence that defendant Kristy Ross ever designed a system scan advertisement. Excerpts from the chat log demonstrate that Ms. Ross relied on other IMI employees for technical assistance with creatives. Dec. 11, 2006 log, (FTC024977, RDX 10; December 12, 2006 log, FTC024980, RDX 11; December 18, 2006 log, FTC 024990, RDX 12; March 5, 2007 log, FTC 025085, RDX 13.) Ms. Ross' emails with Mr. Gieron support the fact that she depended on other IMI employees for technical assistance. (Gieron Depo., RDX 1, pp. 91:1-6; 153:1-7; KRG9, RDX 14, p. 8; KRG13, RDX 15, pp. 11 and

13, KRG, RDX 6, p. 3; FTC11, RDX 16, p. 5-6; KRG4, RDX 17, p. 4.) Mr. Gieron recognized that there was zero evidence that Ms. Ross exerted any control over the ads. (Gieron Depo., RDX 1, pp. 196:18-25-197:1-6; 266:1-16.) What the evidence actually establishes is that the overwhelming majority of the ads which were the subject of the Gieron deposition may have been annoying, but did not contain deceptive attributes or false statements and that the single ad that the FTC cites to support the assertion that Ms. Ross placed an ad with a scanning attribute suffers from major evidentiary problems. *See* Response to MF #61 above.

> 64. The Defendants copied the look and feel of Microsoft Windows, including the trademark Microsoft Security Shield for their system scan advertisements. Declaration of Microsoft Trademark Paralegal Jennifer Bollen, Vol. VI, Ex. 59, p. 171, ¶9; #launch, Vol. VII, Ex. 74, pp. 346-347; D.E. #3 (Ex. 17), D'Souza Counterclaim, pp. 96-98, ¶106-107; Hurd Decl., Vol. I, Ex. 22, p. 44, ¶3; Marcynzsyn Decl., Vol. I, Ex. 30, p. 59, ¶4.

RESPONSE: MF #64 states that "defendants copied the 'look and feel' of Microsoft Windows . . . ." There is no evidence that defendant Kristy Ross ever designed an ad that copied the "look and feel" of a Microsoft ad, much less a system scan advertisement. Indeed, the facts are to the contrary. (Gieron Depo., RDX 1, pp. 196:18-25; 197:1-6; 266:1-16.) What the evidence actually establishes is that the overwhelming majority of the ads which were the subject of the Gieron deposition may have been annoying, but did not contain deceptive attributes or false statements and that the single ad that the FTC cites to support the assertion that Ms. Ross placed an ad with a scanning attribute suffers from major evidentiary problems. *See* Response to MF # 61 above.

> 65. Defendant Ross opened and managed more than 50 accounts with MyGeek which disseminated these types of advertisements for at least an 18 month period displaying well over 600 million impressions to consumers across thousands of web sites on the Internet. Ex. 3 to Gieron Depo., Vol. VIII, Ex. 87, pp. 84-85.

RESPONSE: MF #65 misconstrues the record. MF #65 cites to a chart introduced during Mr. Gieron's deposition of accounts opened by Kristy Ross and the number of

impressions for those accounts. By referencing "these types of advertisements," MF #65 attempts to create the impression that Ms. Ross placed ads with My Geek / AdOn similar to the ads discussed in the preceding MFs. However, MF #65 fails to cite to a single exhibit from Mr. Gieron's deposition which include dozens of examples of screen shots of ads discussed during Mr. Gieron's deposition. These screen shots reveal that the overwhelming majority of these ads have never even been alleged to have issues with fake scanning. (Gieron Depo., RDX 1, pp. 257:15-18; 258:21-25; 259:1-4; 275:13-16; 289:22-25; 419:10-21; 421:6-8; 422:6-9; 441:7-13; 445:20-24.) That the one ad discussed at Mr. Gieron's deposition with a scanner function suffered from major evidentiary issues. *See* Response to MF # 61 above. MF #65 also attempts to create the impression that because Ms. Ross had a number of accounts with My Geek there was something untoward about Ms. Ross's relationship with My Geek. Mr. Gieron offered no such testimony.

66. The FTC has received over 1,300 consumer complaints about the Defendants' products and advertising. MF #16.

RESPONSE: MF#66 misstates the record in that it refers to "Defendants' products and advertising," because the overwhelming majority of consumer complaints appear to have been directed towards products with which the FTC's own investigator asserts Ms. Ross had no connection. (Drexler Dec., ¶ 110., FTC Vol. XII, Ex. 103 attachment A, pp. 28-30)

67. Consumers have also described their negative experiences with the Defendants on Internet forums and chat rooms. D.E. #3 (Ex. 20), Drexler Decl., p. 8, ¶27.

RESPONSE: *See* Response to MF # 66.

68. Consumers describe seeing the Defendants' dire warning messages indicating that a problem exists on their computers, that their computers are infected with viruses, or that their computers are compromised. Belobraydic Decl., Vol. I, Ex. 4, p. 11, ¶2; Cherup Decl., Vol. I, Ex. 5, p. 12, ¶3; Church Decl., Vol. I, Ex. 6, p. 13, ¶2; Cucura Decl., Vol. I, Ex. 7, p. 16, ¶2; avis Decl., Vol. I, Ex. 8, p. 18, ¶2; Dubois Decl., Vol. I, Ex. 9, p. 20, ¶3; Eykelhoff Decl., Vol. I, Ex. 10, p. 22, ¶2; Fichana Decl., Vol. I, Ex. 11, p. 24, ¶2;

Fletcher Decl., Vol. I, Ex. 13, p. 28, ¶2; Foster Decl., Vol. I, Ex. 14, p. 29, ¶2; Golden Decl., Vol. I, Ex. 16, p. 33, ¶2; Harris Decl., Vol. I, Ex. 18, p. 36, ¶2; Hodge Decl., Vol. I, Ex. 20, p. 41, ¶3, Keasling Decl., Vol. I, Ex. 23, p. 47, ¶2; Kilby Decl., Vol. I, Ex. 24, p. 49, ¶2; Kilthau Decl., Vol. I, Ex. 25, p. 50, ¶2; Layton Decl., Vol. I, Ex. 26, p. 52, ¶9; Levens Decl., Vol. I, Ex. 27, p. 54, ¶3; Lovell Decl., Vol. I, Ex. 29, p. 57, ¶4; Martin Decl., Vol. I, Ex. 31, p. 62, ¶2; Mullen Decl., Vol. I, Ex. 32, p. 64, ¶2; Myers Decl., Vol. I, Ex. 33, p. 66, ¶2; Phelan Decl., Vol. I, Ex. 37, p. 71, ¶2; Pritchett Decl., Vol. I, Ex. 39, p. 74, ¶2; Roberts Decl., Vol. I, Ex. 43, p. 81, ¶3; Stalvey Decl., Vol. I, Ex. 46, p. 86, ¶2; Welander Decl., Vol. I, Ex. 50, p. 93, ¶2.

RESPONSE: *See* Response to MF # 66.

69. Consumers then report that they are urged to, and do in fact, purchase one of Defendants' security products in order to remedy the critical threats detected by the Defendants' scanner, only to learn later that they have been duped. Belobraydic Decl., Vol. I, Ex. 4, p. 11, ¶2; Church Decl., Vol. I, Ex. 6, p. 13, ¶4; Cucura Decl., Vol. I, Ex. 7, p. 16, ¶3; Eykelhoff Decl., Vol. I, Ex. 10, p. 22, ¶2; Fletcher Decl., Vol. I, Ex. 13, p. 28, ¶3; Foster Decl., Vol. I, Ex. 14, p. 29, ¶2; Furney Decl., Vol. I, Ex. 15, p. 30, ¶3; Golden Decl., Vol. I, Ex. 16, p. 33, ¶2; Harris Decl., Vol. I, Ex. 18, p. 36, ¶2; Hunt Decl., Vol. I, Ex. 21, p. 43, ¶2; Hurd Decl., Vol. I, Ex. 22, p. 44, ¶3; Kilby Decl., Vol. I, Ex. 24, p. 49, ¶2; Kilthau Decl., Vol. I, Ex. 25, p. 50, ¶2; Lovell Decl., Vol. I, Ex. 29, p. 57, ¶4; Martin Decl., Vol. I, Ex. 31, p. 62, ¶2; Marcynzsyn Decl., Vol. I, Ex. 30, p. 59, ¶4; Myers Decl., Vol. I, Ex. 33, p. 66, ¶2; Phelan Decl., Vol. I, Ex. 37, p. 71, ¶2; Oswald Decl., Vol. I, Ex. 35, p. 68, ¶3; Pritchett Decl., Vol. I, Ex. 39, p. 74, ¶2; Stalvey Decl., Vol. I, Ex. 46, p. 86, ¶2; Randall Decl., Vol. I, Ex. 40, p. 76, ¶5; Richgels Decl., Vol. I, Ex. 42, p. 80, ¶2; Thompson Decl., Vol. I, Ex. 48, p. 89, ¶4; White Decl., Vol. I, Ex. 51, p. 95, ¶3.

RESPONSE: *See* Response to MF # 66.

70. The FTC has obtained 51 declarations from consumers describing their experiences with 47 of the Defendants' products marketed using the techniques described in MF # 68-69, including "Winfixer," "Antivirus XP," "AntiVirus 2008," "SystemDoctor," "DriveCleaner," "AdvancedCleaner," "Antivirus XP 2008," "WinAntiVirus," "WinAntiSpyware," "InternetAntispy," ErrorProtector," and "ErrorSafe." Consumer Declarations, Vol. I, Ex. 3-53, pp. 10-101; Novick Decl., Ex. 103, Vol. XII, p.13-15, ¶4.

RESPONSE: *See* Response to MF # 66.

71. Consumer Shane Levens, who worked as a Network Systems Administrator for Harvard College Libraries and who is a certified Microsoft Systems Engineer, saw a new window spawn in his Internet browser (a "pop up") for "Winfixer 2005" while surfing the Internet in the fall of 2005. Levens Decl., Vol. I, Ex. 27, p. 54, ¶3.

72. The pop up window Levens saw appeared to be an official Microsoft operating system error warning claiming that his computer was in danger and that he should run a

scan. Levens Decl., Vol. I, Ex. 27, p. 54, ¶3.

73. Because of Levens' experience and training, he recognized that this was not actually a Microsoft warning, but had a very difficult time closing the pop up. Levens Decl., Vol. I, Ex. 27, p. 54, ¶3.

74. Each time Levens would try to exit, more pop ups would appear, and he finally had to use the windows task manager to exit out of the pop up without downloading any files. Levens Decl., Vol. I, Ex. 27, p. 54, ¶3.

75. Because Levens was concerned that the average computer user would not be able to exit out of the endless pop ups without possibly downloading something, he filed a complaint.

RESPONSE: *See* Response to MF # 71.

76. Tim Dubois is another consumer who saw "Winfixer 2005" pop ups in the fall of 2005. Dubois Decl., Vol. I, Ex. 9, p. 20, ¶3.

77. Dubois thought the Winfixer 2005 pop ups looked like legitimate Microsoft notifications telling him that his computer was infected. Dubois Decl., Vol. I, Ex. 9, p. 20, ¶3.

78. The ads told Dubois to download Winfixer to scan his computer for errors. Dubois Decl., Vol. I, Ex. 9, p. 20, ¶3.

79. Dubois received the pop ups incessantly for about two weeks, at which point he was forced to erase his entire hard drive just to remove the Winfixer pop ups from his computer. Dubois Decl., Vol. I, Ex. 9, p. 20, ¶3.

80. Although Dubois tried to contact the Defendants by using the email address provided on their WinFixer.com website, he never received any response. Dubois Decl., Vol. I, Ex. 9, p. 20, ¶3.

81. The Defendants' Advanced Cleaner fake scan ad purports to detect pornography on consumers' computers and then proceeds to display a series of hardcore pornographic images that supposedly exist on the scanned computers. D.E. #3 , (Ex. 20), Drexler Decl., pp. 53-57; D.E. #3 (Ex. 13) Nolet Decl., p. 2; Mullen Decl., Vol. I, Ex. 32, p. 64, ¶2; Renteria Decl., Vol. I, Ex. 41, p. 78, ¶5; Woerner Decl., Vol. I, Ex. 53, pp. 99-101; Graham Decl., Vol. I, Ex. 17, p. 35, ¶2.

RESPONSE: MF #81 misstates the evidence. MF #81 states "defendant' advanced cleaner fake scan ad purports to detect pornography…" There is no evidence that defendant Kristy Ross ever created, designed, or placed an advertisement for AdvancedCleaner, which is

the advertisement referenced in MF #81. The facts are to the contrary. (D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30; Drexler Dec., ¶ 110.) The MF fails to cite to the Gieron deposition in which Mr. Gieron states that the screenshots at Para. 24 of the FTC complaint never ran at MyGeek/AdOn, that he had no recollection that the Advanced Cleaner ad depicted at p. 9 of the FTC complaint running at MyGeek/AdOn or, indeed, of *any* AdvancedCleaner ads running at the MyGeek/AdOn network (Gieron Depo., RDX 1, pp. 442:12-25; 443:1-3.)

82. Kent Woerner, the Network Administrator for Unified School District 273 in Beloit, Kansas, came across one of the Defendants' AdvancedCleaner ads in March 2008. Woerner Decl., Vol. I, Ex. 53, p. 99, ¶2.

RESPONSE: MF #82 states that Kent Woerner came across one of "Defendants" AdvancedCleaner ads". There is no evidence that defendant Kristy Ross ever created, designed, or placed an advertisement for AdvancedCleaner. The facts are to the contrary. (D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30; Drexler Dec., ¶ 110.) *See* Response to MF # 81 above.

83. Woerner was alerted when a female student using a sixth grade classroom computer was exposed to pornographic images, which were displayed as part of a pop-up advertisement that purported to scan the computer the student was using. Woerner Decl., Vol. I, Ex. 53, p. 99, ¶¶2 - 3.

RESPONSE: *See* Response to MF # 81 above.

84. When Woerner consulted the log file history for the computer, he discovered that the Defendants' *advancedcleaner.com* website was the source of the advertisement. Woerner Decl., Vol. I, Ex. 53, p. 99, ¶5.

RESPONSE: MF #84 refers to "Defendant' advancedcleaner.com website" There is no evidence that Kristy Ross has ever been associated with the advancedcleaner.com website. *See* Response to MF # 81 above.

85. Woerner visited the website and viewed the advertisement which did in fact appear to be a scan of the computer. Woerner Decl., Vol. I, Ex. 53, p. 99, ¶6.
RESPONSE: *See* Response to MF # 81 above.

86. The ad Woerner saw featured a bar that went across the screen that simulated a

scanner, depicting files that the scanner was purportedly checking, and every few minutes pornographic pictures appeared with text that said these pictures were found on the computer, including an image of a woman performing oral sex. The scanner also said that it found viruses and spyware on the computer. Woerner Decl., Vol. I, Ex. 53, p. 99, ¶6.

RESPONSE: *See* Response to MF # 81 above.

87. At the conclusion of the scan, the advertisement urged Woerner to purchase the Defendants' AdvancedCleaner product to remove the pornography detected on the computer. Woerner Decl., Vol. I, Ex. 53, p. 99, ¶8.

RESPONSE: *See* Response to MF # 81 above.

88. Woerner searched the hard drive of the computer for the pornographic images the scanner claimed were present on the computer, but found nothing. Woerner Decl., Vol. I, Ex. 53, p. 99, ¶9.

RESPONSE: *See* Response to MF # 81 above.

89. Woerner then ran antivirus software on the computer, which indicated that the computer was not infected with viruses or spyware. Woerner Decl., Vol. I, Ex. 53, p. 99, ¶9.

RESPONSE: *See* Response to MF # 81 above.

90. Woerner then went to the exact same URL the student viewed on two other school computers, the workstation in his office and the filtering server, and received the exact same pop up advertisement with the exact same scan. Woerner Decl., Vol. I, Ex. 53, p. 100, ¶10.

RESPONSE: *See* Response to MF # 81 above.

91. The Advanced Cleaner ad scan Woerner saw calculated the exact same number of pornographic pictures no matter which computer upon which it ran. Woerner Decl., Vol. I, Ex. 53, p. 100, ¶10.

RESPONSE: *See* Response to MF # 81 above.

92. Woerner had earlier suspected that the pop up advertisement was just an animation and not really a true scan, and his tests on the other two computers confirmed his suspicion. Woerner Decl., Vol. I, Ex. 53, p. 100, ¶11.

RESPONSE: *See* Response to MF # 81 above.

93. Consumer Joe Renteria observed an unsolicited Internet Explorer window appear

on his screen and display a scan of his computer. Renteria Decl., Vol. I, Ex. 41, p. 78, ¶5.

RESPONSE: *See* Response to MF # 81 above.

94. The scan Renteria saw showed various pornographic images, and claimed that the images resided on his computer. Renteria Decl., Vol. I, Ex. 41, p. 78, ¶5.

RESPONSE: *See* Response to MF # 81 above.

95. At the conclusion of the scan, Renteria was urged to download Defendants' AdvancedCleaner product to remove the pornographic images detected on his computer. Renteria Decl., Vol. I, Ex. 41, p. 78, ¶6.

RESPONSE: MF #95 refers to "Defendants' AdvancedCleaner product." There is no evidence that defendant Kristy Ross was associated with the development of the AdvancedCleaner product or ever ran ads for the product. *See* Response to MF # 81 above.

96. As an experienced web designer, Renteria recognized the scan as nothing more than an animated image displayed in his web browser and proceeded to file a complaint with one of the FTC's law enforcement partners. Renteria Decl., Vol. I, Ex. 41, p. 78, ¶7.

RESPONSE: *See* Response to MF # 81 above.

97. Within his complaint, Renteria included the URL of the AdvancedCleaner scan that he saw. Renteria Decl., Vol. I, Ex. 41, p. 78, ¶7.

RESPONSE: *See* Response to MF # 81 above.

98. FTC investigator Novick and online advertising industry veteran Michiel Nolet later visited this URL, which is part of the Defendants' *advancedcleaner.com* website. D.E. #3 (Ex. 20), Drexler Decl., pp. 53-57, D.E. #3 (Ex. 13). Nolet Decl., p. 2.

RESPONSE: MF #98 refers to "Defendants' advancedcleaner.com website" There is no evidence that defendant Kristy Ross has ever been associated with the advancedcleaner.com website. *See* Response to MF # 81 above.

99. Both Novick and Nolet saw the exact same bogus system scan reported by Renteria, and have both independently verified Renteria's conclusion that the scan is fake. D.E. #3 (Ex. 20), Drexler Decl., pp. 53-57; D.E. #3 (Ex. 13), Nolet Decl., p. 2.

RESPONSE: *See* Response to MF # 81 above.

100. In February 2008, consumer John Graham also received a pop up ad for Advanced Cleaner while using his computer. Graham Decl., Vol. I, Ex. 17, p. 35, ¶2.

RESPONSE: *See* Response to MF # 81 above.

101. The ad Graham saw showed a picture of a bare-breasted woman with the text, "If we can see what you are doing, anyone can." The pop up also stated, "Illegal content found at your pc! Explicit content on your pc may lead to..." and then listed various embarrassing results. Graham Decl., Vol. I, Ex. 17, p. 35, ¶2.

RESPONSE: *See* Response to MF # 81 above.

102. Graham said the pop up stated that if he bought Advanced Cleaner for $39.95, the program would rid his computer of illegal content. Graham Decl., Vol. I, Ex. 17, p. 35, ¶2.

RESPONSE: *See* Response to MF # 81 above.

103. Neither Graham nor his wife, the only two users of the computer, store pornographic or illegal content on their computer, and as a result were able to identify the scan as fake. Graham Decl., Vol. I, Ex. 17, p. 35, ¶4.

RESPONSE: *See* Response to MF # 81 above.

104. As a result, the Grahams promptly filed a complaint with one of the FTC's law enforcement partners. Graham Decl., Vol. I, Ex. 17, p. 35, ¶5.

RESPONSE: *See* Response to MF # 81 above.

105. In March 2008, consumer Cynthia Randall was surfing the Internet when she was redirected to a website she did not enter into her browser. Randall Decl., Vol. I, Ex. 40, p. 76, ¶2.

RESPONSE: MF # 105 refers to Ms. Randall's declaration. Ms. Randall, as noted below, complained about XP Antivirus 2008. There is no evidence that Kristy Ross was associated with XP Antivirus 2008. In fact, the FTC's investigator, Ms. Novick, testified in her Declaration that Ms. Ross was not associated with Antivirus 2008. (Drexler Dec., ¶ 110; D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30.)

106. This webpage commenced a scan of Randall's computer and purported to detect several viruses as well as out-of-date anti-virus software. Randall Decl., Vol. I, Ex. 40, p. 76, ¶3.

RESPONSE: *See* Response to MF # 105 above.

107. The webpage then urged Randall to purchase Defendants' XP Antivirus 2008 program in order to remove the infection. Randall Decl., Vol. I, Ex. 40, p. 76, ¶4.

RESPONSE: MF #107 refers to "Defendants' XP Antivirus 2008 program". There is no evidence that defendant Kristy Ross was associated with the XP 2008 Antivirus program. *See* Response to MF # 105 above.

108. Randall recognized that the color scheme and appearance of the scanner matched Microsoft Windows, and assumed that the scan was conducted by a Microsoft product. Randall Decl., Vol. I, Ex. 40, p. 76, ¶5.

RESPONSE: *See* Response to MF # 105 above.

109. To protect her computer, Randall proceeded to purchase XP Antivirus 2008 for $49.95 using her credit card. Randall Decl., Vol. I, Ex. 40, p. 76, ¶6.

RESPONSE: *See* Response to MF # 105 above.

110. When Randall attempted to download XP Antivirus 2008, nothing happened and she never received the product. Randall Decl., Vol. I, Ex. 40, p. 76, ¶7.

RESPONSE: *See* Response to MF # 105 above.

111. Uncertain about how to proceed, Randall conducted an Internet search for XP Antivirus 2008 and found numerous consumer complaints calling the product a scam. Randall Decl., Vol. I, Ex. 40, p. 76, ¶8.

RESPONSE: *See* Response to MF # 105 above.

112. Randall then called her credit card company to inquire about the charge, but was informed that the charge had already been processed. Randall Decl., Vol. I, Ex. 40, p. 76, ¶9.

RESPONSE: *See* Response to MF # 105 above.

113. Randall never received a refund or credit for XP Antivirus 2008. Randall Decl., Vol. I, Ex. 40, p. 76, ¶9.

RESPONSE: *See* Response to MF # 105 above.

114. Roberta Cucura also saw pop ups for XP Antivirus in May 2008 and thought that

the warning messages were from Microsoft because they had the Microsoft shield logo. Cucura Decl., Vol. I, Ex. 7, p. 16, ¶3.

RESPONSE: MF #114 refers to Ms. Cucura's complaint about XP Antivirus. There is no evidence to suggest that Kristy Ross ever was associated with XP Antivirus. In fact, the FTC's investigator, Ms. Novick, testified in her Declaration that Ms. Ross was not associated with XP Antivirus. (Drexler Dec., ¶ 110; D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30.)

115. The pop ups warned Cucura that her computer was infected with viruses. Cucura Decl., Vol. I, Ex. 7, p. 16, ¶3.

RESPONSE: *See* Response to MF # 114 above.

116. Cucura ran the free virus scan that the Defendants offered and, believing it was a Microsoft product, bought the XP Antivirus software for $49.95 to get rid of the viruses from her computer. Cucura Decl., Vol. I, Ex. 7, p. 16, ¶3.

RESPONSE: MF #116 refers to the "free virus scan that Defendants offered". There is no evidence that defendant Kristy Ross ever offered XP Antivirus software for sale or ever was associated with XP Antivirus. *See* Response to MF # 114 above.

117. However, after being charged $105 for a bundle of software that she did not agree to purchase, Cucura asked her bank to refund her money and provide her with the phone number for the company responsible for the product. Cucura Decl., Vol. I, Ex. 7, p. 16, ¶4.

RESPONSE: *See* Response to MF # 114 above.

118. Despite more than 20 phone calls, Cucura was never able to get through to the company because the voicemail box was always full. Cucura Decl., Vol. I, Ex. 7, p. 16, ¶5.

RESPONSE: *See* Response to MF # 114 above.

119. Cucura also continued to receive XP Antivirus pop ups and, after speaking with a computer repair technician, was only able to rid herself of them by buying a new computer. Cucura Decl., Vol. I, Ex. 7, p. 16, ¶6.

RESPONSE: *See* Response to MF # 114 above.

120. In approximately August 2008, Stephen Layton received a pop up message in the

middle of his desktop that said "Antivirus XP 2008." Layton Decl., Vol. I, Ex. 26, p. 52, ¶6.

RESPONSE: MF #120 refers to Ms. Cucura's complaint about Antivirus XP 2008. There is no evidence to suggest that Kristy Ross ever was associated with Antivirus XP 2008. In fact, the FTC's investigator, Ms. Novick, testified in her Declaration that Ms. Ross was not associated with Antivirus XP 2008. (Drexler Dec., ¶ 110; D.E. 186-3, FTC Vol. XII, Ex. 103, pp. 28-30.)

121. It appeared to have scanned Layton's computer and it said that he had thousands of viruses it had identified on his computer, and warned him that he would have serious consequences if he did not remove the viruses. Layton Decl., Vol. I, Ex. 26, p. 52, ¶10.

RESPONSE: *See* Response to MF # 120 above.

122. When Layton attempted to close the pop up box, he was redirected to the Antivirus XP website. Layton Decl., Vol. I, Ex. 26, p. 52, ¶11.

RESPONSE: *See* Response to MF # 120 above.

123. Layton ran McAfee and Spybot Search and Destroy anti-virus software products and neither detected any of the phantom viruses that Antivirus XP claimed to exist. Layton Decl., Vol. I, Ex. 26, p. 52, ¶12.

RESPONSE: *See* Response to MF # 120 above.

124. Layton did not want to purchase Antivirus XP, but could not find a way to remove the disruptive program from his computer. Layton Decl., Vol. I, Ex. 26, p. 52, ¶13-16.

RESPONSE: *See* Response to MF # 120 above.

125. Layton eventually replaced the computer entirely to rid himself of the Antivirus XP software. Layton Decl., Vol. I, Ex. 26, p. 52, ¶17.

RESPONSE: *See* Response to MF # 120 above.

125.5 In addition to consumers Randall, Cucura and Layton, 16 other consumer declarants report that Defendants' ads were confusingly similar or identical to official Microsoft Windows notifications. These complaints cover the following products: Winfixer, AVSystemCare, WinAntispyware, DriveCleaner, AntiVirus 2009 Pro, SpyBurner, WinSpywareProtect, AntiVirus XP, PerformanceOptimizer, WinAntivirus Pro, WinXProtector, WinSpyware, AntiVirus 2008, PowerAntivirus 2009, and

CryptDrive. MF # 56.

RESPONSE: MF #125.5 refers to consumer complaints about "defendants' ads" for a series of products. The evidence is clear that only products in this list for which Kristy Ross may have ever placed ads were Winfixer and DriveCleaner. (Drexler Dec., ¶ 110; D.E. 186-3, FTC Vol. XII, Ex. 103, pp. 28-30.) The MF fails to cite to the Gieron deposition and exhibits FTC Vol. VII Ex. 87, which actually contained examples of the ads Ms. Ross may have placed with the MyGeek/AdOn network for Winfixer and Drivecleaner. There is no evidence that these are the ads that customers viewed and identified as "confusingly similar or identical to official Microsoft Widows notifications."

126. Consumers report seeing pop ups for defendants' DriveCleaner software claiming that errors, spyware, and pornography resided on their computers. Belobraydic Decl., Vol. I, Ex. 4, p. 11, ¶2; Fieler Decl., Vol. 1, Ex. 12, p. 26, ¶3; Small Decl., Vol., I, Ex. 45, p. 85, ¶2.

RESPONSE: MF# 126 refers to "defendants' Drivecleaner software". Although there is information that defendant Ross placed ads for DriveCleaner through the MyGeek/AdOn network (D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30) there is no evidence that she had any role in the development of this software or that the ads she placed for DriveCleaner exhibited the same functionality as that described by the consumers listed in MF# 126. Indeed, Mr. Gieron specifically stated that he had no recollection of ads with pornography running for globedat. (Gieron Depo., RDX 1, p. 442:17-20.)

127. Cheryl Belobraydic received a pop up ad in April 2008 warning her that her computer was infected with spyware. Belobraydic Decl., Vol. I, Ex. 4, p. 11, ¶2.

RESPONSE: *See* Response to MF # 126 above.

128. Belobraydic states that the pop up looked like it was from McAfee and said she needed to upgrade her antivirus software. Belobraydic Decl., Vol. I, Ex. 4, p. 11, ¶2.

RESPONSE: *See* Response to MF # 126 above.

129. As a result, Belobraydic clicked on the pop up, and was redirected to a web site where she could purchase a product called "DriveCleaner." Belobraydic Decl., Vol. I, Ex. 4, p. 11, ¶2.

RESPONSE: *See* Response to MF # 126 above.

130. Believing that DriveCleaner was a McAfee product, Belobraydic purchased the software. Belobraydic Decl., Vol. I, Ex. 4, p. 11, ¶3.

RESPONSE: *See* Response to MF # 126 above.

131. However, after downloading DriveCleaner, Belobraydic's computer became unusable and she had to seek assistance from a technologist to remove DriveCleaner from her computer. Belobraydic Decl., Vol. I, Ex. 4, p. 11, ¶3.

RESPONSE: *See* Response to MF # 126 above.

132. The Defendants marketed numerous products in this fashion. Novick Decl., Vol. XII, Ex. 103, pp.13-15, ¶4; MF ## 68-69.

RESPONSE: MF #132 states "defendants marketed numerous products in this fashion" referring, it seems, to the description of Ms. Cheryl Belobraydic's experience as described in MFs ##127-131. There is no evidence that Ms. Ross marketed any products in this fashion. The FTC has developed information as to which products Ms. Ross may have advertised on the MyGeek/AdOn network. (D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30.) Copies of ads that may have been placed by Ms. Ross are included in D.E. #186-3, FTC Vol. VIII Ex. 87. There is no evidence that these ads functioned as described by the consumers referred to in MF #132.

133. AdvancedCleaner is one of many privacy protection products Defendants marketed and sold to the public by using advertisements that display an elaborate system scan that purports to detect pornographic files on scanned computers. D.E. #3 (Ex. 20), Drexler Decl., pp. 53-57, ¶¶164 - 169, 175; Mullen Decl., Vol. I, Ex. 32, p. 64, ¶2; Renteria Decl., Vol. I, Ex. 41, p. 78, ¶5, Woerner Decl., Vol. I, Ex. 53, pp. 99-101; Graham Decl., Vol. I, Ex. 17, p. 35, ¶2.

RESPONSE: MF #133 states that "AdvancedCleaner is one of the many privacy protection products Defendants marketed and sold to the public…" There is no evidence that

defendant Kristy Ross ever created, designed, or placed an advertisement for AdvancedCleaner or that she ever "marketed and sold" AdvancedCleaner to the public or that she ever was associated with AdvancedCleaner in any capacity. The evidence is to the contrary. In fact, the FTC's investigator, Ms. Novick, testified in her Declaration that Ms. Ross was not associated AdvancedCleaner. (Drexler Dec., ¶ 110; D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30.)

The MF fails to cite to the Gieron deposition in which Mr. Gieron states that the screenshots at Para. 24 of the FTC complaint never ran at MyGeek/AdOn, that he had no recollection that the Advanced Cleaner ad depicted at p. 9 of the FTC complaint running at MyGeek/AdOn or, indeed, of *any* AdvancedCleaner ads running at the MyGeek/AdOn network. (Gieron Depo., RDX 1, pp. 442:12-25; 443:1-3.)

134. By visiting the URL provided to the FTC in the consumer complaint filed by Joe Renteria (see MF # 97), FTC Investigator Novick was able to view and capture the unsolicited AdvancedCleaner advertisement Renteria witnessed on his computer. D.E. #3 (Ex. 20), Drexler Decl., pp. 54-57, ¶¶166-168.

RESPONSE: *See* Response to MF # 133 above.

135. The Defendants claim in their Advanced Cleaner ad that "[i]llegal porn content" exists on the computer "scanned" by the ad. D.E. #3 (Ex. 20), Drexler Decl., p. 55, ¶168.

RESPONSE: *See* Response to MF # 133 above.

136. In their Advanced Cleaner ad, the Defendants display a series of pornographic images under the heading "[t]hreats observed" along with the folder locations where these pictures purportedly reside. D.E. #3 (Ex. 20), Drexler Decl., pp. 54-55, ¶167.

RESPONSE: *See* Response to MF # 133 above.

137. In their Advanced Cleaner ad, the Defendants make a variety of claims under the heading "Scan Results," including the representation that the scan detected 21 "Porn Movies" and 146 "Adult Pictures." D.E. #3 (Ex. 20, Att. HH), Drexler Decl., p. 68.

RESPONSE: *See* Response to MF # 133 above.

138. None of the pornographic pictures purportedly detected in the Defendants' Advanced Cleaner advertisement actually exist on the "scanned" computer. D.E. #3 (Ex.

20), Drexler Decl., pp. 56-57, ¶170 - 175.

RESPONSE: *See* Response to MF # 133 above.

139. The entire "scan" conducted in the Defendants' ad consists of nothing more than a movie displayed in the viewer's Internet browser, and as a result, the scanner displays the exact same results each time it runs, regardless of which computer the ad is displayed upon. D.E. #3 (Ex. 20), Drexler Decl., p. 57, ¶175. This is true even on the FTC's Internet Lab computers, which are reset before each use to a pristine, "out of the box" state and contain no pornographic files of any kind. D.E. #3 (Ex. 20), Drexler Decl., p. 57, ¶175.

RESPONSE: MF # 139 is referring to a product called AdvancedCleaner. There is no evidence that defendant Kristy Ross ever created, designed, or placed an advertisement for AdvancedCleaner or that she ever "marketed and sold" AdvancedCleaner to the public or that she ever was associated with AdvancedCleaner in any capacity. The evidence is to the contrary. In fact, the FTC's investigator, Ms. Novick, testified in her Declaration that Ms. Ross was not associated AdvancedCleaner. (Drexler Dec., ¶ 110; D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30.) The MF fails to cite to the Gieron deposition in which Mr. Gieron states that the screenshots at Para. 24 of the FTC complaint never ran at MyGeek/AdOn, that he had no recollection that the Advanced Cleaner ad depicted at p. 9 of the FTC complaint running at MyGeek/AdOn or, indeed, of *any* AdvancedCleaner ads running at the MyGeek/AdOn network. (Gieron Depo., RDX1, pp. 442:12-25; 443:1-3.)

140. The advertisement pictured above is but one of an arsenal of similar ads that resided on Defendants' *advancedcleaner.com* website. D.E. #3 (Ex. 20), Drexler Decl., pp. 55-56, ¶169.

RESPONSE: *See* Response to MF # 139 above.

141. While these ads differ in appearance, they all rely on the same deceptive marketing technique – false statements about explicit/pornographic content allegedly detected on the "scanned" computer. D.E. #3 (Ex. 20), Drexler Decl., pp. 55-56, ¶169.

RESPONSE: *See* Response to MF # 139 above.

142. Many of these ads include photographs of graphic depictions of sexual activities that purportedly exist on the scanned computer. D.E. #3 (Ex. 20), Drexler Decl., pp. 55-56, ¶169.

RESPONSE: *See* Response to MF # 139 above.

143. The screenshots of more than 15 of these advertisements are attached to FTC Investigator Novick's declaration and when viewed from the same computer one after another, the ads contradict each other, and report wildly different numbers of pornographic files "detected" on the exact same computer. D.E. #3 (Ex. 20), Drexler Decl., pp. 55-56, ¶169.

RESPONSE: *See* Response to MF # 139 above.

144. In Investigator Novick's screenshots, the first AdvancedCleaner ad displays a series of pornographic pictures purportedly found on the scanned computer and informs the viewer that there are "156 pornographic files in your system." D.E. #3 (Ex. 20), Drexler Decl., pp. 55-56, ¶169.

RESPONSE: *See* Response to MF # 139 above.

145. The second AdvancedCleaner ad Investigator Novick saw "locates" and displays an entirely different set of explicit pictures and informs the viewer that it detected a total of 44 pornographic files on the scanned computer. D.E. #3 (Ex. 20), Drexler Decl., pp. 55-56, ¶169.

RESPONSE: *See* Response to MF # 139 above.

146. The third Advanced Cleaner advertisement Investigator Novick saw contradicts both of the findings in MF ## 144-145, by "locating" and displaying yet another series of explicit pictures and claiming that 316 "compromising" and "Internet track" files exist on the computer. D.E. #3 (Ex. 20), Drexler Decl., pp. 55-56, ¶169.

RESPONSE: *See* Response to MF # 139 above.

147. Investigator Novick found 15 other Advanced Cleaner advertisements that acted similarly to the ads described in MF ## 144-146. D.E. #3 (Ex. 20), Drexler Decl., p. 55, ¶169.

RESPONSE: *See* Response to MF # 139 above.

148. DriveCleaner is another security product marketed by the Defendants through deceptive advertising. D.E. #3 (Ex. 20), Drexler Decl., pp. 62-68, ¶¶187 - 203; Myers Decl., Vol. I, Ex. 33, p. 66, ¶¶2 - 4; Small Decl., Vol. I, Ex. 45, p. 85, ¶¶2 - 4; Belobraydic Decl., Vol. I, Ex. 4, p. 11, ¶2; Fieler Decl., Vol. 1, Ex. 12, p. 26, ¶3.

RESPONSE: MF #148 misstates the evidence. MF #148 states that "DriveCleaner is another security product marketed by the Defendants through deceptive advertising". Although there is evidence that defendant Ross placed ads for DriveCleaner through the MyGeek/AdOn network, D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30, the evidence does not establish that Ms. Ross placed a deceptive ad for DriveCleaner that was viewed by US consumers. *See* Response to MF # 61 above.

149. DriveCleaner is promoted by Defendants as a product that will "[e]rase all compromising evidence" from consumers' computers. D.E. #3 (Ex. 20), Drexler Decl., p.66, ¶197.

RESPONSE: The citations contained in MF #149 do not support the asserted fact. The paragraph describes the procedures Ms. Drexler followed on October 30, 2008 when she accessed a link for Drivecleaner. Because this test was not done during the time frame that Ms. Ross placed ads for DriveCleaner through the MyGeek/AdOn network, there is no evidence that the ads that Drexler described are the ads that Ms. Ross placed to market DriveCleaner to consumers. (Gieron Depo., RDX 1, pp. 201:6-19; 202:13-20.)

150. By reviewing consumer complaints that include the URL of the DriveCleaner advertisement consumers saw, and by following links posted by a security researcher who has tracked the progression of Defendants' deceptive ads, FTC Investigator Novick was able to review a series of Defendants' DriveCleaner advertisements that were in wide circulation on the Internet. D.E. #3 (Ex. 20), Drexler Decl., pp. 62-63, 65-6, ¶¶188, ¶¶196 - 98.

RESPONSE: The citations contained in MF #150 do not support the asserted fact. The paragraph citations describes the procedures Ms. Drexler followed on October 30, 2008, when she accessed links for Drivecleaner. Because this test was not done during the time frame that Ms. Ross placed ads for DriveCleaner through the MyGeek/AdOn network, there is no evidence that the ads that Drexler described are the ads that Ms. Ross placed to market DriveCleaner to consumers. (Gieron Depo., RDX 1, pp. 201:6-19; 202:13-20.)

151. The Defendants' ads for DriveCleaner purport to scan consumers' computers and detect "Adult," "Pornographic." "Sensitive," or "Compromising" files. D.E. #3 (Ex. 20), Drexler Decl., pp. 62-63, 65-66, ¶¶188, ¶¶196 - 98.

RESPONSE: MF #151 describes what "defendants' ads" for DriveCleaner purport to do. The citations contained in MF #151 do not support the asserted fact. The paragraph citations describes the procedures Ms. Drexler followed on October 30, 2008, when she accessed links for Drivecleaner. Because this test was not done during the time frame that Ms. Ross placed ads for DriveCleaner through the MyGeek/AdOn network, there is no evidence that the ads that Drexler described are the ads that Ms. Ross placed to market DriveCleaner to consumers. (Gieron Depo., RDX 1, pp. 201:6-19; 202:13-20.)

152. Defendants urge consumers who see their DriveCleaner ads to download and purchase the program in order to remove the files detected during the scan. D.E. #3 (Ex. 20), Drexler Decl., pp. 63-64, ¶190; Myers Decl., Vol. I, Ex. 33, p. 66, ¶¶2 - 4; Small Decl., Vol. I, Ex. 45, p. 85, ¶¶2 - 4.

RESPONSE: MF #152 states that "Defendants' urge consumers who see their DriveCleaner ads to download and purchase the program…" The citations contained in MF #152 do not support the asserted fact. The paragraph describes the procedures Ms. Drexler followed on May 11, 2007 when she accessed links for Drivecleaner. Because this test was not done during the time frame that Ms. Ross placed ads for DriveCleaner through the MyGeek/AdOn network, there is no evidence that the ads that Drexler described are the ads that Ms. Ross placed to market DriveCleaner to consumers. (Gieron Depo., RDX 1, pp. 201:6-19; 202:13-20.)

153. All of the representations in Defendants' advertisement are false because no actual scan occurred and the ad "detects" the same number of files no matter which computer it runs on. D.E. #3 (Ex. 20), Drexler Decl., pp., 67, 68, ¶¶199, 202 - 03.

RESPONSE: MF #153 states "all of the representations in Defendants' advertisement are false because no actual scan occurred…" The citations contained in MF #153 do not support

the asserted fact. The paragraphs describe the procedures Ms. Drexler followed on May 11, 2007 and November 21, 2007 when she accessed links for Drivecleaner. Because this test was not done during the time frame that Ms. Ross placed ads for DriveCleaner through the MyGeek/AdOn network, there is no evidence that the ads that Drexler described are the ads that Ms. Ross placed to market DriveCleaner to consumers. (Gieron Depo., RDX1, pp. 201:6-19; 202:13-20.)

154. Investigator Novick captured this same exact advertisement detecting the same "948 dangerous files" on at least seven different occasions at various locations within the Defendants' websites. Novick Decl., Vol. XII, Ex. 103, pp.15-16, ¶6.

RESPONSE: MF #154 refers to "defendants' websites." However, there is no evidence that defendant Kristy Ross was associated with the Drivecleaner website.

155. In other DriveCleaner ads, like the one pictured below, Defendants purport to have detected 179 visits to "Adult websites" and 21 visits to "Illegal websites," including "*getlaid.com*," "*gayanalsex.com*," and "*asianteens.net*." D.E. #3 (Ex. 20), Drexler Decl., p. 65, ¶194.

RESPONSE: MF #155 states that on DriveCleaner ads such as that depicted below, "Defendants purport to have detected…" The citations contained in MF #155 do not support the asserted fact. The paragraph describes the procedures Ms. Drexler followed on November 21, 2007 when she accessed links for Drivecleaner. Because this test was not done during the time frame that Ms. Ross placed ads for DriveCleaner through the MyGeek/AdOn network, there is no evidence that the ads that Drexler described are the ads that Ms. Ross placed to market DriveCleaner to consumers. (Gieron Depo., RDX 1, pp. 201:6-19; 202:13-20.)

156. These representations are false because no scan has occurred and the "adult" and "illegal" sites displayed in the ad never change, regardless of which computer the ad is displayed upon, including the pristine computers within the FTC's Internet Lab. " D.E. #3 (Ex. 20), Drexler Decl., pp. 67-68, ¶¶200 - 203.

RESPONSE: *See* Response to MF # 155 above.

157. WinAntiVirus is one of many antivirus products marketed by the Defendants. D.E. #3 (Ex. 20), Drexler Decl., pp. 57-62, ¶¶176 - 186.

RESPONSE: MF #157 misstates the evidence. MF #157 states that "WinAntiVirus is one of many antivirus products marketed by the Defendants." Although there is evidence that defendant Ross placed ads for WinAntiVirus through the MyGeek/AdOn network , D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30, the evidence does not establish that Ms. Ross placed any deceptive ad for WinAntiVirus. *See* Response to MF # 61 above.

158. FTC Investigator Novick reviewed multiple WinAntiVirus advertisements hosted on *amaena.com*, the IMI-owned website that was named in many consumer complaints as one of the sources of Defendants' advertising. D.E. #3 (Ex. 20), Drexler Decl., pp. 57-60, ¶¶176 - 181; Davis Decl., Vol. I, Ex. 8, pp. 18-19; Marcynzsyn Decl., Vol. I, Ex. 30, pp. 59-62.

RESPONSE: MF #157 misstates the evidence. In addition, there is not any evidence that Ms. Ross had any connection with the website amaena.com. *See* Response to MF # 66 above.

159. Each of the WinAntiVirus advertisements hosted on *amaena.com* contains misrepresentations about the security status of the computer on which the ad is displayed. D.E. #3 (Ex. 20), Drexler Decl., pp. 57-62, ¶¶176 - 186.

RESPONSE: MF #159 misstates the evidence. MF #159 states that "[e]ach of the WinAntiVirus advertisements hosted on *amaena.com* contains misrepresentations." Although there is evidence that defendant Ross placed ads for WinAntiVirus through the MyGeek/AdOn network, D.E.# 186-3, FTC Vol. XII, Ex. 103, pp. 28-30, the evidence does not establish that Ms. Ross placed any deceptive ad for WinAntiVirus nor is there any evidence that Ms. Ross had any connection with the website amaena.com. *See* Response to MF # 61 above. Moreover, the tests performed by Drexler that were the source of these conclusions took place on May 11, 2007. Drexler Decl., p59, ¶179. Because this test was not done during the time frame that Ms. Ross placed ads for WinAntivirus through the MyGeek/AdOn network, there is no evidence that

the ads that Drexler described are the ads that Ms. Ross placed to market WinAntivirus to consumers. (Gieron Depo., RDX 1, pp. 201:6-19; 202:13-20.)

160. One of these ads informs viewers "WARNING: YOUR CURRENT ANTIVIRUS PROTECTION IS NOT EFFECTIVE!" It also states that "your system is currently sending private information and documents to a remote computer." D.E. #3 (Ex. 20), Drexler Decl., p. 60, ¶¶181.

RESPONSE: *See* Response to MF # 159 above.

161. Consumers who attempt to close this window see another pop-up window with the ominous warning "NOTICE: You have not completed the scan. There is a security vulnerability from the Serwab. We recommend you DOWNLOAD one of the security software programs to prevent malware infections." D.E. #3 (Ex. 20), Drexler Decl., p. 60, ¶¶181.

RESPONSE: *See* Response to MF # 159 above.

162. The representations in the advertisement above, as well as the follow up pop-up window, are false because the advertisement detects the same purported vulnerabilities no matter which computer it is displayed upon, including the pristine computers within the FTC's Internet lab. D.E. #3 (Ex. 20), Drexler Decl., pp. 61-62, ¶¶182- 86.

RESPONSE: *See* Response to MF # 159 above.

163. The warning "YOUR CURRENT ANTIVIRUS IS NOT EFFECTIVE" is displayed even on computers running the latest versions of legitimate antivirus software, including Symantec Antivirus, which is installed on the FTC Internet lab computers used to view the advertisements. D.E. #3 (Ex. 20), Drexler Decl., pp. 60, 62, ¶181, 186.

RESPONSE: *See* Response to MF # 159 above.

164. In addition to their bogus virus scans, several of Defendants' WinAntivirus advertisements misappropriate the "look and feel" of the Microsoft Windows XP Security Center, a program bundled with Microsoft Windows XP that runs automatically and notifies consumers when their security settings put them at risk. Declaration of Microsoft Trademark Paralegal Jennifer Bollen, Vol. VI, Ex. 59, pp. 171-172, ¶¶9-11; D.E. #3 (Ex. 20), Drexler Decl., p. 61, ¶182.

RESPONSE: *See* Response to MF # 159 above.

165. By copying portions of the official Windows XP Security Center – including the "Security Center: Help Protect your PC" logo, the Windows XP Security Center "shield," and the "Resources" list in the left column, Defendants dupe consumers into believing that Windows itself has detected a problem with their computer and is urging them to

purchase Defendants' software. D.E. #3 (Ex. 20), Drexler Decl., p. 61, ¶¶182-183; Declaration of Microsoft Trademark Paralegal Jennifer Bollen, Vol. VI, Ex. 59, p. 171, ¶9, MF #242; #launch, Vol. VII, Ex. 74, p. 346-47.

RESPONSE: *See* Response to MF # 159 above.

166. Internet advertising agency MyGeek retained copies of some of the Defendants' ads that were placed through accounts created by Kristy Ross. MF # 52.

RESPONSE: MF #166 refers to MF #52 which in turn refers to Exhibits 13-15, 20 and 23 from the deposition of MyGeek/AdOn representative, Geoff Gieron. Mr. Gieron's deposition did not establish that the ads pictured in the exhibits were ads belonging to or made by defendant Kristy Ross. In fact, Mr. Gieron's deposition established the opposite. For example, referring to the ads depicted at EX 13, Mr. Gieron made it clear that it is not the URL that controls the content of the ads but the server of the ad:

> Q: But at the server level, so it means that a computer [somewhere][2] that is making the ad is what is responsible for the content of that?
> A: It's returning content, correct.
> Q: And do you have any information whatsoever or knowledge that Kristy Ross was the person who was in control of a server for the Winfixer product?
> A: I do not.
> Q: Do you have any information whatsoever that Kristy Ross was an individual in charge for a WinAntivirus product?
> A: No.
> Q: Ever at any time?
> A: No.
> (Gieron Depo., RDX 1, pp. 266:3-16.)

Nor did Mr. Gieron's deposition even establish that the ads pictured were placed by Ms. Ross. Taking the Exhibits in order:

FTC 13: Screen shots and URLs come from individuals at Hotbar. Gieron Depo., RDX 1, pp. 92: 13-25; 93:1-20. The appearance of the ad in the screenshots was not the same as the way Gieron viewed the ads that he reviewed from Ms. Ross. Gieron Depo, RDX 1, pp. 94:2-4;

94:24-25; 95:1-21. Mr. Gieron was not even certain the ad in question came from one of Ms. Ross' accounts. He thought the ad was "probably" associated with Ms. Ross' account based on the appearance of code in the URL. (Gieron Depo., RDX 1, pp. 97: 8-16.)

FTC 14: Mr. Gieron testified that he had reviewed the ad pictured in this exhibit. (Gieron Depo., RDX 1, p. 99:21-25.) But he was not asked about whether this was Ms. Ross' ad or if it was identified to an account opened by Ms. Ross. (Gieron Depo, RDX 1, pp. 100-102.)

FTC 15: Mr. Gieron could not confirm that he had reviewed this ad, just that he had reviewed ads that were similar. (Gieron Depo., RDX 1, p. 103: 11-17.) Gieron stated that someone on his team had seen the pictured ad while checking URLs specific to Ms. Ross OR the URLs of other accounts in the system OR accounts of a similar nature. (Gieron Depo., RDX 1, p. 105:16-18.) Gieron identifies the ad pictured in Ex. 15 to Ms. Ross because of code contained in the URL was similar to codes in ads he received from Ms. Ross. (Gieron Depo., RDX 1, p. 106:17-23.) When Mr. Gieron forwarded a copy of the ad that is pictured to Ms. Ross, Ms. Ross' responded that she would try to send new links to help resolve the problem. D.E. #186-3, Gieron (Depo. Ex., Vol. VIII, Ex. 87, FTC 15, p. 1.)

FTC 20: Mr. Gieron did not see the boxes referenced at p. 1-2 of FTC 20. Rather these were ad behaviors reported to him by his traffic partners. (Gieron Depo, RDX 1, p. 125:13-24.) Nor did Mr. Gieron see the box in the ad on p. 3 of FTC Ex. 20. (Gieron Depo., RDX 1, p. 126:5-12.) Instead, the ad Mr. Gieron saw (that was *not the same* as the screen shots in p. 1-3 of FTC 15), was the same content as an ad placed by Ms. Ross. However, Mr. Gieron could not state that the URL designation of the ad was coming from Ms. Ross. (Gieron Depo., RDX 1, p. 126:20-24.) Moreover, it seems that AdOn cannot locate the ad in question in their system. The

---

[2] The text reads "somewhat" but that appears to be an error.

ad located on p. 286 is an ad that traffic partner Mike Romoff inquires of his contacts at MyGeek/AdOn after viewing the ad. He asks his contacts at MyGeek AdOn to try to locate the ad on their advertising system. The MYGeek /AdOn employee, after checking into the matter writes back, "We're still looking to find either of these vendors but can't find them in our system. We've had our DBA scan all landing URLs for either of the domains, but don't see it". (D.E. #186-3, Gieron Depo. Ex., Vol. VIII, Ex. 87, p. 286.) This response would actually indicate that this was not an ad placed by Kristy Ross. Indeed, Mr. Gieron admitted that he was unable to state with certainty that the URL that appears on p.3 of FTC 20 was a link that Ms. Ross sent to him Gieron Depo., RDX 1, p. 331:9-13, and admitted that AdOn was even having difficulty identifying the ad that the traffic partners were complaining about in the AdOn system. (Gieron Depo., RDX 1, pp. 332:11-25; 333:1-7.)

FTC 23: Mr. Gieron stated with respect to the ads shown at p. 2-3 of FTC 23 that he saw how the ads should look but that he had not viewed the ads from the standpoint of a user. (Gieron Depo., RDX 1, p. 137:19-22.) Mr. Gieron identifies these ads to Ms. Ross based on certain code designations that appear in the URL. (Gieron Depo., RDX 1, p. 138:5-10.) Mr. Gieron was not able to state with certainty that the way that the ad appeared at p. 2-3 of FTC 23 was how the page appeared all the time (Gieron Depo., RDX 1, p. 145:16-19.) Consequently, Gieron made clear; "So what a US consumer saw, where and when, I couldn't give you a guarantee." (Gieron Depo., RDX 1, pp. 145:25; 146:1.) Gieron described the ad at p. 2-3 of FTC 23 as the page that was seen and captured by AdOn employee Rachel Greenberg. (Gieron Depo., RDX 1, p. 145: 22-23.) Mr. Gieron stated that the ads pictured at p. 2-3 of FTC 23 were the ads that were put into two of Kristy's accounts. (Gieron Depo., RDX 1, p. 146:5-9.) However, on examination by the defense, Mr. Gieron admitted that the links that AdOn launched were *not the same links* as

those tested by AdOn employee Greenberg. The links Kristy sends to AdOn, KRG 27, RDX 5, p. 5, are the same links that Ryan emails to Kristy saying ready to launch, KRG 27, RDX 5, p. 11, but not the same as the links Rachel Greenberg tested at KRG27, RDX 5, p. 20-21. In fact, Gieron confirmed there was a discrepancy in the links:

> A: I can't tell you which one was activated on the network though.
>
> Q: What do you –
>
> A: So you're asking me to be able to see into my database the time that this all happened, which was linked, without accounting for human error and passing information on a – on anything else.

(Gieron Depo., RDX 1, p. 354: 15-21.)

> A: Yes. The link that Rachel put on top of a screen shot did not match. That was not the link taken from the system. So how she lost those two symbols, I can't tell you.

(Gieron Depo., RDX 1, pp. 356: 23-25; 357:1.)

> 167. Two of these ads for WinAntiVirus are nearly identical to ones that Investigator Novick found on the *amaena.com* and *winantivirus.com* web sites. Ex. 18 to Gieron Depo., Vol. VIII, Ex. 87, p. 274; Ex. 20 to Gieron Depo., Vol. VIII, Ex. 87, p. 286.
>
> **RESPONSE:** The ad on p. 274 is an ad viewed by MyGeek traffic partner Lee Tankersley, but which has not been established to have been placed by Kristy Ross. Indeed, Mr. Gieron testified that he could not recall the structure of this ad as being the one submitted by Ms. Ross or that he reviewed. Gieron Depo., RDX 1, p. 111:2-25. The ad on p. 286 could not be attributed to either Ms. Ross, or even to the AdOn system. *See* references to FTC Ex #20 in Response to MF # 166 above.
>
> Furthermore, the FTC MF#167 asserts that the ads in FTC Ex. 18 and 20 are "nearly identical" to ads viewed by FTC Investigator Novick. The FTC fails to provide a cite so that one might determine which ads Novick viewed that the FTC contends were similar. The Declaration of Sheryl Drexler (Novick) refers to her review of Winantivirus ads at paragraphs 179-181 and

references exhibits LL, MM and JJ. Each of these ads differ in critical respects from the ads depicted in FTC 18 and FTC 20. Moreover, as Mr. Gieron made clear in his deposition, it is not a valid exercise to view ad content on a web site months after the ads you are trying to document and to assume that the appearance would be the same. Gieron stated that if you were to look at a link today you would not know how it looked back at the time it originally ran. (Gieron Depo., RDX 1, p. 396: 6-9, 17-20.) Instead, Mr. Gieron testified, to know how a link appeared to someone at a particular time, you would need to be in that time frame or have screen shots from that time frame. (Gieron Depo., RDX 1, pp. 396: 22-25; 397:1-2.)

168. Investigator Novick found WinAntiVirus ads on the *amaena.com* and *winantivirus.com* websites. Novick Decl., Vol. XII, Ex. 103, p. 16, ¶7; D.E. #3 (Ex. 20), Drexler Decl., p. 60, ¶181.

RESPONSE: *See* Response to MF # 167 above.

169. The Defendants created numerous static image advertisements that warned consumers of critical errors on their computers, and submitted those files to advertising networks, like ValueClick, to display across the Internet. Ex. 9 to Webster Depo., Vol. 6, Ex. 57, pp. 126-139.

RESPONSE: There is no evidence that Kristy Ross submitted any ads to the ValueClick ad network. In fact the evidence is to the contrary, for the ValueClick representative testified that Ms. Ross did not place ads with the ValueClick ad network. (D.E. #186-3, Webster Depo., Vol.VI, Ex. 57, pp. 68-69.) In addition, there is evidence that Ms. Ross refused to approve a static gif advertisement contained within the IRC chat logs. On Dec 7, 2006, FTC 024970, RDX 19, fuzzy[3] and leo75 have another interchange in which fuzzy notices a series if gif files in her MyGeek template. She asks in no uncertain terms that they be removed:

[3]The FTC has not established that all of the chat messages sent under the name "fuzzy" were sent by Kristy Ross. Nevertheless, because throughout its summary judgment papers the FTC attributes all of the statements of "fuzzy" to Ms. Ross, additional statement by "fuzzy" are included here for completeness.

<leo75> Kristy
<leo75> I see in mygeek template
<leo75> errorprotector-epp0-ctx)-s1-wj)-en.gif…
<fuzzy> ok
<fuzzy> we should get those out
<leo75> its ok?
<fuzzy> they shouldn't be there
<fuzzy> no
<leo75> hm there reason for mgcog4 traffic :(
<fuzzy> not sure why no one else saw that but
<fuzzy> : (
<fuzzy> yes we should remove them>
<leo75> ok

170. The Defendants, using the name, Revenue Response, uploaded their fake error message ads to the ValueClick advertising network, and ValueClick confirmed that these fake error message ads were displayed more than one billion times. D'Souza Aff., Vol. X, Ex. 97, p. 76, ¶131; Rebuttal Report of Michiel Nolet, Vol. VI, Ex. 58, pp. 162-163; Novick Decl., Vol. XII, Ex. 103, pp.16-17, ¶8.

RESPONSE: *See* Response to MF # 169 above.

171. FTC expert Kevin Johnson analyzed hundreds of the Defendants' fake error message ads and found that they were nothing more than static images, which had no ability to conduct a scan of a consumers' computer or determine if an error existed. Expert Report of Kevin Johnson, Vol. VI, Ex. 63, pp. 493-494.

RESPONSE: MF# 171 fails to point out that the static image ads upon which Mr. Johnson based these opinions were obtained through the ValuClick network and are not identified to Kristy Ross. There is no evidence that Kristy Ross submitted any ads to the ValueClick ad network. In fact the evidence is to the contrary. (D.E. #186-3, Webster Depo., Vol.VI, Ex. 57, pp. 68-69.) In addition, there is evidence that Ms. Ross refused to approve a static gif advertisement contained within the IRC chat logs. *See* Response to MF # 169 above.

172. FTC expert Michiel Nolet reviewed the Defendants' fake error message ads and concluded that the ads were "static image[s] that [were] completely incapable of executing any code." Rebuttal Report of Michiel Nolet, Vol. VI, Ex. 58, p. 162.

RESPONSE: MF# 172 fails to point out that the static image ads upon which Mr. Nolet based his opinion were obtained through the ValueClick network and are not identified to Kristy Ross. There is no evidence that Kristy Ross submitted any ads to the ValueClick ad network. In fact the evidence is to the contrary. (D.E. 186-3, Webster Depo., Vol.VI, Ex. 57, pp. 68-69.) In addition, there is evidence that Ms. Ross refused to approve a static gif advertisement contained within the IRC chat logs. *See* Response to MF # 169 above.

173. After reviewing the Defendants' fake error messages, Nolet concluded that "there is absolutely no way in which the creative could be aware of any sort of error on my computer." Rebuttal Report of Michiel Nolet, Vol. VI, Ex. 58, p. 162.

RESPONSE: *See* Response to MF # 172 above.

174. Nolet and Johnson's findings as described in MF ## 171-173 were confirmed by defense expert Daniel Kim, who acknowledged that the defendants' static image ads were incapable of scanning a consumer's computer and detecting errors. Kim Depo, Vol. VII, Ex. 86, p. 462 (184:16-20).

RESPONSE: *See* Response to MF ## 171 and 172 above.

175. In a number of the campaigns run by the Defendants, every one of the displayed ads purported to detect errors and none of the ads reported that "no error was detected." Ex. 9 to Webster Depo., Vol. 6, Ex. 57, pp. 126-139.

RESPONSE: MF #175 refers to "campaigns run by the defendants." The referenced ads were placed through the ValueClick advertising network. There is no evidence that Kristy Ross submitted any ads to the ValueClick ad network. In fact the evidence is to the contrary. (D.E. 186-3, Webster Depo., Vol.VI, Ex. 57, pp. 68-69.) In addition, there is evidence that Ms. Ross refused to approve a static gif advertisement contained within the IRC chat logs. *See* Response to MF # 169 above.

176. Kim testified that the Defendants' ads could have been displayed based on an independent computer scan was conducted by code originating from ValueClick's server. Kim Depo., Vol. VII, Ex. 86, pp. 470-472 (216:17 - 221:18).

RESPONSE: MF #176 refers to "Defendants' ads." The ads referred to were placed through the ValueClick advertising network and the unrebutted evidence establishes that Ms. Ross did not, in fact, submit any ads to the ValueClick ad network. *See* Response to MF # 169 above.

177. Kim testified that the Defendants' ads could have been targeted only to users with out-of-date web browsers or operating system based on the information supplied in the "user agent" – a string of data that is transmitted by all Internet browsers that reveals the operating system and web browser of the user. Kim Depo., Vol. VII, Ex. 86, pp. 470-472 (216:17 - 221:18).

178. Kim could not provide any evidence to support the theories described in MF ## 176-177. Kim Depo., Vol. VII, Ex. 86, p. 467 (202:7 - 204:20).

179. Rodney Webster, for ValueClick, testified that he conclusively ruled out both of the theories described in MF ## 176-177 and testified that the Defendants' fake error ads were indiscriminately targeted to users throughout the United States and abroad. Webster Depo., Vol. VI, Ex. 57, p. 61 (73:15 - 73:23; 74:19 - 74:22; 75:8 - 75:14) 62 (77:10 - 77:23; 78:19 - 79:3; 80:23 - 81:8); 68 (101:22 - 102:12).

RESPONSE: MF #179 refers to "Defendants' fake error ads". The ads referred to were placed through the ValueClick advertising network. There is no evidence that Kristy Ross submitted any ads to the ValueClick ad network. In fact the evidence is to the contrary. *See* Response to MF # 169 above.

180. Both Johnson and Nolet reviewed the data provided by Webster and agreed with Webster's conclusion as described in MF # 179. Rebuttal Report of Kevin Johnson, Vol. VI, Ex. 64, pp. 510-511; Rebuttal Report of Michiel Nolet, Vol. VI, Ex. 58, pp. 160-163.

RESPONSE: MF#180 fails to point out that the alleged ads upon which Mr. Johnson and Mr. Nolet based their opinion were not placed by Kristy Ross. *See* Response to MF # 169 above.

181. A Flash object is a binary file that can contain multiple graphics and logic to animate those graphics. The file can then be opened by a Flash player plug-in within a consumer's browser much like a word document can be opened in Microsoft Word. Johnson Depo., Vol. VII, Ex. 67, p. 170 (70:4 - 70:18), 171 (74:9 - 74:17).

182. FTC expert Kevin Johnson reviewed and analyzed 21 Flash objects uploaded to the ValueClick network by the defendants. Expert Report of Kevin Johnson, Vol. VI, Ex. 63, p. 494.

RESPONSE: There is no evidence that Kristy Ross submitted any ads to the ValueClick ad network. In fact the evidence is to the contrary. *See* Response to MF # 169 above.

183. Johnson explained in his expert report that one of the flash objects he examined was a fake system scan animation that displayed a list of Windows files it was purportedly scanning and concluded with a warning that dangerous files had been found. Expert Report of Kevin Johnson, Vol. VI, Ex. 63, p. 494.

RESPONSE: MF # 183 fails to point out that the alleged ads upon which Mr. Johnson based his opinion were not placed by Kristy Ross. *See* Response to MF # 169 above.

184. Johnson stated in his expert report that the animation was incapable of conducting any scan, and was nothing more than a movie that reaches the same result every time it is played. Expert Report of Kevin Johnson, Vol. VI, Ex. 63, pp. 495-496.

RESPONSE: *See* Response to MF # 183 above.

185. Johnson viewed the advertisements on a computer running the Linux operating system, but the animation purported to scan a variety of Microsoft Windows files that do not exist on a Linux machine. Expert Report of Kevin Johnson, Vol. VI, Ex. 63, p. 495.

RESPONSE: *See* Response to MF # 183 above.

186. As a technical administrator for IMI, Defendant James Reno kept logs of all online "chat" conversations among IMI employees. Reno Decl., D.E. #69 (Ex. 3), ¶¶4-6.

187. The Defendants' chat logs are real time conversations that the Defendants recorded, preserved, and used for different areas of specialty in the company. Reno Decl., D.E. #69 (Ex. 3), ¶¶4-6.

188. The Defendants used different channels for their separate chats including, but not limited to channels for the launch of products, call center employees, and for the system administrators. #sysadmin, Vol. VII, Ex. 79, #sm, Vol. VII, Ex. 80, #launch, Vol. VII, Ex. 74, #mc Vol. VII, Ex. 73, #support, Vol. VII, Ex. 83, #ohio, Vol. VII, Ex. 82.

189. The Defendants admit to using Microsoft Windows trademarks in their advertisements in order to frighten consumers. #launch, Vol. VII, Ex. 74, p. 346-47.

RESPONSE: MF #189 misstates the evidence. MF #189 claims that in a specified section of IRC chat "defendants admitted to using Microsoft Windows trademarks in their advertisements in order to frighten consumers." The only entries by fuzzy in this section of log state that they have 30 creatives for errorclean and to just add aggression to them. ***Nowhere*** is there an admission by defendant Ross as to use of Microsoft trademarks to frighten consumers.

190. Defendant Sam Jain explains in a chat that he wants to use "warning/scary style" creatives for their product ErrorClean. #launch, Vol. VII, Ex. 74, p. 346-47; Novick Decl., Vol. XII, Ex. 103, pp. 13-15, ¶4.

191. In a chat, IMI employees discuss with Defendant Jain where they can find Microsoft Windows creatives to steal, and one employee says to look at http://support.microsoft.com/gp/securityhome. #launch, Vol. VII, Ex. 74, p. 346-47.

RESPONSE: The cited section does not support this assertion, but instead reveals that defendant Ross does not participate in this section of the conversation. Moreover, the chat log also does not suggest that IMI employees sought to steal Microsoft creates. Rather, in the chat logs, <ak> states "examples – windows security center" and <mike> "should have some warning style as they have been requested." Nowhere in the chat log does anyone discuss stealing Microsoft creatives.

192. An IMI employee explains in a chat with Defendant Jain that there is an entire "Fake Windows" folder located on one of the defendants' servers. #launch, Vol. VII, Ex. 74, p. 346-47.

193. In early 2006, Microsoft's trademark enforcement group became aware that the Defendants were using Microsoft's trademarks on the *amaena.com* website, which hosted hundreds of the defendants' ads. Declaration of Microsoft Trademark Paralegal Jennifer Bollen, Vol. VI, Ex. 59, p. 171, ¶9; D.E. #3 (Ex. 20), Drexler Decl., p.58, ¶¶177-183.

RESPONSE: MF #193 misstates the evidence. MF # 193 claims that "Microsoft's trademark enforcement group became aware that the Defendants were using Microsoft's trademarks. . . ." Microsoft drew no conclusion about who was using the trademarks. Further,

there is no evidence whatsoever to suggest that the amaena.com site was registered to Ms. Ross or that she controlled the content of this site.

194. *Amaena.com* was registered with false information, but Microsoft was able to determine that the website belonged to the defendants. Declaration of Microsoft Trademark Paralegal Jennifer Bollen, Vol. VI, Ex. 59, p. 171, ¶9.

RESPONSE: *See* Response to MF # 193 above.

195. Microsoft's Trademark Team sent a demand letter to defendant James Reno informing him that *amaena.com* features advertisements "purporting to be warnings that [consumers'] computers have been infected with spyware" and that "encourage consumers to purchase alleged anti-spyware software." The Trademark Team further stated "this site is making use of our Security Shield trademark in a manner that is virtually identical to Microsoft's use...and create[s] the false impression that these products are sponsored or endorsed by Microsoft." Declaration of Microsoft Trademark Paralegal Jennifer Bollen, Vol. VI, Ex. 59, p. 172, ¶11.

RESPONSE: *See* Response to MF # 193 above.

196. Reno promptly forwarded Microsoft's email to defendants Jain and Sundin, who responded by instructing Reno to lie to Microsoft and tell the company that he has contacted his "client" to resolve the issue. Reno email, Vol. VII, Ex. 72, p. 286-88.

RESPONSE: *See* Response to MF # 193 above. Moreover, it is interesting to note that Mr. Reno allegedly forwarded this email to defendants Jain and Sundin, but not to Ms. Ross, who the FTC claims was a partner at IMI. Mr. Reno's decision to not include Ms. Ross in this alleged discussion about threats from Microsoft undermines the FTC's claims about Ms. Ross's importance at IMI, as it is reasonable to assume that litigation threats from the largest software company in the world would be a topic that would be disseminated to all partners of any company.

197. Defendant Ross is frequently asked to review and approve advertisements for the defendants' scareware products. #launch, Vol. VII, Ex. 74, p. 346-352.

RESPONSE: MF #197 misstates the evidence in this case. The cited logs do not support the assertion that Ms. Ross frequently was asked to review and approve advertisements.

First, at Vol. VII, Ex. 74, p. 346, "fuzzy" (the screen name that the FTC attributes to Ms. Ross), does not appear at all. On p. 347 fuzzy's only contribution to the conversation, which is taking place among ak, mike, sam and leo75, is to say they have some 30 creatives for errclean and to ask that aggression be added to them. She does not approve anything. Significantly, on this same page, it is clear that an individual logging as <mike> is in charge of making the creative for errclean. Specifically, ak writes: "mike, when could we have the 2-3 creatives for errclean approx" to which mike responds, "I'll put high priority on them for them and have em tomorrow."

At p. 348, fuzzy does not approve an advertisement, but to the contrary, points out that certain ads cannot be used either because they are misleading or too graphic. Specifically, at p. 348 , fuzzy points out to leo75 (who, unlike Ms. Ross, evidently has some role in the content of the ads), that one ad says "your current antivirus is not effective" to which fuzzy cautions, "you can't say that." (D.E. #186-3, #launch , Vol. VII, Ex. 74, p. 348.) Also at p. 348 and into the next page of the log (which is not included by the FTC), fuzzy asks leo75 where a particular as for pcprivacytool is running. (D.E. #186-3, #launch, Vol. VII, Ex. 74, pp. 348-349.) When Leo75 tells her "mostly USA," fuzzy logs, "we can't use that for RON that shows a nipple in it maybe dieter can run it, but we can't so let's get that ad redone without no nudity." (D.E. #186-3, #launch , Vol. VII, Ex. 74, pp. 348-349.) Fuzzy continues, revising the idea of having dieter run the ad, "actually its best not to run it at all on ron that might upset people and give bad publicity." (D.E. #186-3, #launch , Vol. VII, Ex. 74, pp. 348-349.) At p. 229, FTC 025181, RDX 18, Leo75 asks mike "Mike can we get this creative fixed?"

At p. 349, fuzzy logs that a particular French ad has to be changed because someone named vero says, "it has misspellings, its sloppy errors all over the place. Fuzzy adds that "even

that affiliate says its 'full of mistakes'". Contrary to the FTC assertion, fuzzy does not approve any ads, but instead suggests changes to an ad based on spelling errors or content that she feels is inappropriate. The page is also instructive as proof that ads were run through affiliates which was a source of difficulty in that it allowed others to control the content of certain ads.

At p. 350, fuzzy asks leo75 about a "Sleepsea campaign." Here, Leo75 discusses having ads translated into "French, JP, Spanish," from which it does not even appear that whatever products are here being discussed are even being sold in the US. Fuzzy does state that for the marketing of whatever product they are discussing in these foreign countries that "aggression zero doesn't give sales," but fuzzy does not approve any ads.

At p. 351, mike and leo75 are logging about "these creatives for Dieter GERS channel." Fuzzy reviews ads and with respect to a particular blinking functionality they ask her about responds "yes its fine." However, leo75 again states "conv for Dieter GERS still 0.018-0.02 for mainstream." This exchange seems to be about ads being run in Germany. Additional evidence for the fact that these are non US ads is that at p. 348 when fuzzy discusses dieter, it is in the context of his being outside the US.

At p. 352, there is a conversation about language problems with ads which appear to be French and Spanish. The conversation is about ads not working at all. Fuzzy does not approve anything.

At pp. 253-254, leo75 asks either mike or Kristy about the translation of certain language in an ad and fuzzy makes two suggestions about English grammar. In sum, none of the chat logs cited by the FTC support the assertion that Ms. Ross was frequently asked to and/or did frequently approve advertisements.

198. In one such conversation, Ms. Ross – who uses the alias "fuzzy" – is asked to approve language for the Defendants' DriveCleaner advertisement. #mc, Vol. VII., Ex.

73, p. 326; Reno Decl., D.E. #69 (Ex. 3), ¶¶4-6; Novick Decl., Vol. XII, Ex. 103, pp. 13-15, ¶4.

RESPONSE: The cites contained MF 198 do not support the assertion that Ms. Ross is asked to approve or does approve a DriveCleaner ad. Indeed, the log establishes the opposite as fuzzy writes to "lunch," "I don't even know what that is for what is it for." Moreover, the log comes from June 2007 and Ms. Ross' relationship with MyGeek/AdOn terminated on March 29, 2007. (Gieron Depo., RDX 1, p. 381.) Therefore, Ms. Ross never ran the DriveCleaner ad under discussion as part of any advertising campaign. Furthermore, the Ms. Ross is not being asked to approve an ad in the excerpted log, only to assist with the English language usage. Indeed, fuzzy makes it very clear in her response that she does not know what they are working on or what they are trying to say, and that she is not going to assist them in resolving their issues. In response to "lunch" sending certain text, fuzzy writes, "what landing page what id 'payment system'?" Fuzzy continues "anyway I sure you, mike or shane can fix your text." *See* Response to MF # 205 below.

199. Ross is pitched on an advertisement that is supposed to be "scary" and purports to detect "explicit goods" on the viewers' computer, and Ross instructs her foreign subordinates to allow an American employee to fix the poor grammar in the ad. #mc, Vol. VII., Ex. 73, p. 326.

RESPONSE: MF #199 states that in this IRC excerpt, the same as that discussed in #198 above, that "Ross is pitched on a advertisement that is supposed to be 'scary'….and instructs her foreign subordinates to allow an American employee to fix the poor grammar in the ad." The FTC's description of the cited log is misleading. There is no support for the assertion that Ross is being "pitched" on an ad, which implies that she is reviewing the content or appearance of the ad. Instead, she and mike are being asked to assist with English language usage. As discussed above, fuzzy writes to "lunch" "I don't even know what that is for what is it

for." The excerpt has zero support for the FTC's assertion that Ross is "instructing foreign subordinates". Rather, fuzzy makes it clear in her response that she does not know what they are working on or what they are trying to say, and that she is not going to assist them in resolving their issues. In response to "lunch" sending certain text, fuzzy writes; "what landing page what id 'payment system'?" Fuzzy continues "anyway I sure you, mike or shane can fix your text."

200. Jun 30 14:26:37 <fuzzy> is it supposed to be scary?
Jun 30 14:26:47 <Vinchenso> yes....
Jun 30 14:26:52 <Vinchenso> very scary :)
Jun 30 14:26:59 <Vinchenso> uuuuuuuu....
Jun 30 14:27:01 <Lunch> Here is all text from Lp.
Jun 30 14:27:02 <Lunch> Payment system detected explicit goods which were bought from your PC.
Jun 30 14:27:02 <Lunch> Even if you don't bought the following adult materials, you are not free from
Jun 30 14:27:02 <Lunch> crime responsibility. Clear all payment statistics from your computer.
Jun 30 14:27:23 <fuzzy> what landing page
Jun 30 14:27:31 <fuzzy> what is 'payment system'
Jun 30 14:27:31 <fuzzy> ?
Jun 30 14:27:51 <Vinchenso> fuzzy, this is new creative for [DriveCleaner]
Jun 30 14:27:54 <fuzzy> anyway I assure you, mike or shane can fix your text
Jun 30 14:27:55 <fuzzy> that is not proper
Jun 30 14:27:58 <fuzzy> can you show mike the page
Jun 30 14:28:00 <mike> yeah
Jun 30 14:28:00 <fuzzy> and let him fix I
Jun 30 14:28:02 <fuzzy> he's american
Jun 30 14:28:03 <mike> pls send us the link
Jun 30 14:28:05 <mike> and we can fix it

#mc, Vol. VII., Ex. 73, p. 326.

RESPONSE: Ross's counsel is unsure what the FTC is trying to assert in MF #200. The FTC appears simply to have reproduced a section of the chat log, but does not allege any facts regarding this section. To the extent that the FTC submits this portion of the chat log for the truth of the matter asserted, it is hearsay and should be stricken pursuant to Fed. R. Evid. 802.

201. The chat logs also feature numerous conversations about the mechanics of the defendants' scareware advertisements. #mc, Vol. VII., Ex. 73, p. 337-338, 335, 341;

#launch, Vol. VII., Ex. 74, p. 351; #sm, Vol. VII, Ex. 80, p. 385-388.

RESPONSE: The chat logs do not support the FTC's assertion. *First*, it is critical to note that the FTC offers no information about what product is being advertised in the referenced ads. *Second*, it does not appear that Ms. Ross was involved in these discussions. For example at Vol. VII., Ex. 73, p. 337-338, fuzzy is not involved in the discussion. Mike and leo75 are discussing not wanting the ads "looking wavish" which could be a reference to their desire not to have the ads look like winantivirus. In this exchange mike and leo75 are actually discussing adding language to ensure that the ads are not misleading, including making sure that the example of the scanner states "Typical Scan Results" or "advertisement" because of their recognition that myspace, where the ads are evidently to be run, is a "serious campaign." At p. 335, fuzzy merely asks about the status of some new pages she had requested about which she writes she had already emailed 5 times. At p. 341, mike and pol discuss a gif or flash. Ross is not involved in this conversation. Indeed, elsewhere in the irc logs, there is evidence that Ms. Ross refused to approve a static gif advertisement contained within the IRC chat logs. On Dec 7, 2006, (FTC 024970, RDX 19), fuzzy and leo75 have another interchange in which fuzzy notices a series if gif files in her mygeek template. She asks in no uncertain terms that they be removed:

<leo75> Kristy
<leo75> I see in mygeek template
<leo75> errorprotector-epp0-ctx)-s1-wj)-en.gif…
<fuzzy> ok
<fuzzy> we should get those out
<leo75> its ok?
<fuzzy> they shouldn't be there
<fuzzy> no
<leo75> hm there reason for mgcog4 traffic :(
<fuzzy> not sure why no one else saw that but
<fuzzy> : (
<fuzzy> yes we should remove them>
<leo75> ok

At p. 351, mike and leo75 are logging about "these creatives for Dieter GERS channel". Fuzzy reviews ads and with respect to a particular blinking functionality they ask her about responds "yes its fine". However, leo75 again states "conv for Dieter GERS still 0.018-0.02 for mainstream." This exchange seems to be about ads being run in Germany. Additional evidence for the fact that these are non US ads is that at p. 348 when fuzzy discusses dieter, it is in the context of his being outside the US.

At Ex. 80, pp. 385-388, here is a technical discussion between "mike" "anton" "karthik," "leo75", and "anjali" about an ad with a scanner in which fuzzy does not participate which we know because of an entry on the bottom of Ex. 80, p. 388 in which fuzzy joins at the end of the cited conversations. *See* Response to MF # 205 below.

> 202. The Defendants' chat discussions confirm that the defendants' ads were nothing but elaborate animations that were incapable of conducting any actual system scan. #mc, Vol. VII., Ex. 73, p. 337-338, 335, 341; #launch, Vol. VII., Ex. 74, p. 351; #sm, Vol. VII, Ex. 80, p. 385-388.

RESPONSE: There is nothing in any of these logs that establishes that defendant Ross participated in any discussion which confirmed that the ads were incapable of conducting scans. *See* Response to MF # 201 above for discussion of each page of chat log here cited by the FTC. *See* Response to MF # 205 below.

> 203. Several IMI employees discuss the animation in the advertisements and decide that the animation should be in GIF or Flash format, and should include the words "now scanning," a moving green bar, a time remaining clock, and a number of infections found. #mc, Vol. VII., Ex. 73, p. 341.

RESPONSE: The citations contained in MF #203 do not support the allegations. At p. 341, mike and pol discuss a gif or flash. Ross is not involved in the conversation. Indeed, elsewhere in the irc logs, there is evidence that Ms. Ross instructed gif files to be removed from her ads. On Dec 7, 2006, FTC 024970, RDX 19, fuzzy and leo75 have another interchange in

which fuzzy notices a series if gif files in her mygeek template. She asks in no uncertain terms that they be removed:

<leo75> Kristy
<leo75> I see in mygeek template
<leo75> errorprotector-epp0-ctx)-s1-wj)-en.gif…
<fuzzy> ok
<fuzzy> we should get those out
<leo75> its ok?
<fuzzy> they shouldn't be there
<fuzzy> no
<leo75> hm there reason for mgcog4 traffic :(
<fuzzy> not sure why no one else saw that but
<fuzzy> : (
<fuzzy> yes we should remove them>
<leo75> ok

204. An IMI employee discusses a DriveCleaner advertisement and states that the progress bar and "windows style pop up" are the scanner piece and are both in Flash. #sm, Vol. VII, Ex. 80, p. 385-388.

RESPONSE: MF #204 misstates the evidence because the FTC does not refer to the section of the log in which mike and Karthik (the participants in the log) refer to the third component which is the "Scan now button" "(the download button)." #sm, Vol. VII, Ex. 80, p. 385-388 [OUR CITE FTC 027357, p. 19 of log). This component is significant because it would be the component that was able to download software that would have been capable of performing a scan. *See* Response to MF #205 below.

205. An IMI employee asks another employee for his thoughts on the language in a proposed Drivecleaner ad stating: "Warning!!! Drivecleaner found 948 dangerous files in your system." #sm, Vol. VII, Ex. 80, p. 385-388.

RESPONSE: The log section cited in MF #205 is among other participants and does not include Ms. Ross. Notably, fuzzy does not "join" until the bottom of p. 308, after the time in which the discussion on which the FTC would attempt to rely has terminated. The conversation is hearsay as to Ms. Ross.

206. The exact language described in MF # 205 – complete with the same number of "dangerous objects" has appeared over and over again within DriveCleaner ads captured by the FTC, including as an attachment to Daniel Sundin's affidavit in Canada, in an email between Internet advertising agency MyGeek and Kristy Ross, and as one of the ads viewed by the FTC's investigator on the Defendants' drivecleaner.com website. D.E. #3 (Ex. 20), Drexler Decl., p. 66, ¶197; Ex. D to Sundin Affid., Vol. VIII, Ex. 89, p. 465; Ex. 23 to Gieron Depo., Vol. VIII, Ex. 87, pp. 318-319.

RESPONSE: MF #206 fails to note Mr. Gieron's testimony undermining the allegation that the referenced ads were attributable to Ms. Ross. The MyGeek email referred to in MF #205, that at Gieron Depo., Vol. VIII, Ex. 87, pp. 318-319, was a link that was tested by AdOn employee Rachel Greenberg. Gieron Depo., RDX 1, Vol. VIII, Ex. 87, p. 317. Significantly, however, and Mr. Gieron testified during his deposition, that the screen shots that Ms. Greenberg performed *did not result from the same links to ads placed by Ms. Ross.* (*Compare* Gieron Depo., Vol. VIII, Ex. 87, pp. 318-319 *with* Gieron Depo., Vol. VIII, Ex. 87, pp. 316.) The links to ads sent by Ms. Ross differ by a number of characters from those that appear at pp. 318-319. This means that there is not any conclusive evidence that Ms. Ross ever placed an ad that looked like the DriveCleaner ad referred to in MF #205. Mr. Gieron himself admitted this fact:

> Q: Okay. But the fact remains that this link, the link that is in Rachel's screen shot, doesn't match exactly with what Kristy sent you and what Ryan activated…….
> A: Yes. The link that Rachel put on top of a screen shot did not match. This was not the link taken from the system. So how she lost those two symbols I can't tell you.

(Gieron Depo., RDX 1, pp. 356:7-357:1.) Elsewhere in Mr. Gieron's deposition, he confirmed that even if one or two segments of code in a URL are dropped or changed, this could "absolutely" change everything. (Gieron Depo., RDX 1, pp. 181:18- 183:1.) And while Gieron opines that small changes in a URL would be more likely to cause an error message than a different ad, he ultimately admits that he does not understand code but that every character in a URL has significance. *Id.*

207. The chat logs feature conversations among IMI's customer support center employees. #ohio, Vol.VII, Ex. 82; #support, Vol. VII, Ex. 83; #callcenter, Vol. VII, Ex. 81.

RESPONSE: MF #207 is grounded on hearsay. If offered for the truth of the matter asserted, it should be stricken under Fed. R. Evid. 802. If not offered for the truth of the matter asserted, it is irrelevant and should be stricken under Fed. R. Evid. 402.

208. In the chat logs, the support employees admit that the Defendants' advertisements make false statements and that consumers buy the Defendants' products based on the advertisements' false representations. #ohio, Vol. VII, Ex. 82, p. 408-410; #callcenter, Vol. VII, Ex. 81, p. 402, 405.

RESPONSE: MF #208 refers to two separate IRC logs. Vol. VII, Ex. 82, p.408-410 is an exhibit comprised of page 1601, page 46, and page 1852 of a 1933 log of customer service representatives responding to customer complaints. Vol. VII, Ex. 81, pages 402 and 405 refers to pages 832 and 330 of the 19,212 page log of customer service representatives responding to customer complaints. Kristy Ross does not appear in these pages. None of these 5 individual pages in which customer service representatives comment on products, however, establish that defendant Kristy Ross developed, placed, or was even aware of the specific ads for products referenced therein. *See* Response to MF # 207 above.

209. Cathy Walton, IMI's worldwide call center manager and defendant James Reno's mother, describes a pop up ad she saw from the defendants' MalwareCrush product. #ohio, Vol. VII, Ex. 82, p. 408; CRB, Vol. VII, Ex. 71, p. 281; MF # 346; Novick Decl., Vol. XII, Ex. 103, pp. 13-15, ¶4.

RESPONSE: There is no evidence that defendant Kristy Ross ever created, designed, or placed an advertisement for Malwarecrush. The facts are to the contrary. Indeed, the FTC's investigator Mrs. Novick (nee Drexler) testified in her Declaration that Ms. Ross was not associated with Malwarecrush. (D.E. #3 (Ex. 20), Drexler Dec., ¶ 110; D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30.) The FTC fails to cite to the Gieron deposition and exhibits (FTC Vol.

VII, Ex. 87) which actually contained examples of the ads Ms. Ross may have placed with the MyGeek/AdOn network. These ads do not include any ads for Malwarecrush. *See also* Response to MF # 207 above.

210. Cathy Walton and other IMI employees joke about the MalwareCrush's advertisement and how it deceives consumers:
Feb 05 15:54:03 <msullivan> lol I just got a pop-up for it when I closed the page :P
Feb 05 15:54:34 <cwalton> Yes I did also
Feb 05 15:54:42 <cwalton> your system is in danger
Feb 05 15:54:44 <cwalton> :)
Feb 05 15:54:47 <msullivan> yea..
Feb 05 15:54:50 <msullivan> lol
Feb 05 16:02:00 <tanderson> I love the ones that says your windows registry is infected you should buy now, yet your on linux >_>
Feb 05 16:03:19 <msullivan> yea it's funny.

#ohio, Vol. VII, Ex. 82, p. 408.

RESPONSE: *See* Response to MF # 207 above.

211. A call center employee complains that "the main problem i am dealing with is the scanner versions that won't remove." In response, a second employee states, "that is because it is a scam to get you to buy more stuff. Marketing SUCKS." #ohio, Vol. VII, Ex. 82, p. 410.

RESPONSE: *See* Response to MF # 207.

212. Kristy Ross placed the Defendants' advertisements with Internet advertiser MyGeek. Gieron Depo., Vol. VIII, Ex. 87, p. 9 (31:4 - 31:19), 13 (45:14 - 45:18), 14 (49:20 - 50:9), 33 (128:2 - 30:17).

RESPONSE: The sections of Mr. Gieron's deposition that are cited do not support MF #212. Mr. Gieron testified merely that Globedat was an advertiser in the MyGeek system and that he, Gieron, dealt with and worked directly with Globedat representative Kristy Ross who set up the original advertising accounts. (Gieron Depo., Vol. VIII, Ex. 87, p. 9 (31:4-31:19), 13 (45:14-45:18), 14 (49:20-50:9).) The final section cited (p.33, 128:2-[1]30:17), refers to an email exchange contained at Ex. 87 p. 305-306. In this email exchange, Ryan Maloney sends Ms. Ross screen shots from an ad for winantivirus that contains a number of pop ups. Ms. Ross

responds that it may be an issue with firefox and that she would look into it. Ms. Ross does not deny that this ad was running in her account, but commits to looking into the particular behavior of the ad depicted in the screen shots. Indeed, Mr. Gieron stops short of stating that this particular url was a link sent by Ms. Ross. He simply states that the ad seems by the email string to be traceable back to one of Ms. Ross's accounts:

> Q: Do you know if anyone else – any other advertiser was running that particular URL on page 047370 other than Kristy?
> A: When you say URL, are you talking about the full URL string or WinAntivirus.com?
> Q: the full URL string.
> A: I'm not familiar enough to know that the full URL, who it belongs to. But given the trail of emails, it would lend back to the 55192 account.
> (Gieron Depo., VIII, Ex. 87 p. 34 (130:3-11).)

Critically, even if the FTC had established that the ad Ms. Ross placed exhibited the precise behavior of the ad depicted in Ex. 87 p. 305-306, which it did not, this would not establish that Ms. Ross had placed the type of deceptive, fake scanner ads referred to in the FTC Complaint Paragraphs 15-37. That is because the ad depicted, as with the overwhelming majority of the ads complained about by MyGeek personnel and brought to Ms. Ross' attention did not exhibit fake scanning behavior. Rather, the ads exhibited the aggressive or annoying (but not false or illegal) behavior of running a large number of pop up boxes asking the consumer if they (yes or no) wanted to download certain software. These facts are confirmed with precision in an IRC log between fuzzy and James Reno in which fuzzy admits that certain ads were aggressive but denies that they forced downloads or exhibited other types of arguably deceptive behaviors.

A Jan 9, 2006 conversation between James Reno and fuzzy proceeds as follows: (FTC 039107-109, RDX 20.)

<fuzzy> but as for advertising practices, etc…they aren't illegal, but they are unpleasant sure

<fuzzy> and we are actually looking for alternatives to this that are as productive if not more

<fuzzy> we even have a very major vc firm looking at the company
<fuzzy> that is one of the top 2 in the US
<fuzzy> so they are obviously quite interested…and are fully aware of all ‘issues’ facing the company
<fuzzy> including advertising lawsuits etc….
<james> I think our customer retention sucks : (
<fuzzy> our customer retention does suck
<fuzzy> also in the reorg doc
<fuzzy> and major focus
<james> yep
<fuzzy> we have almost 0 customer retention currently
<fuzzy> I just got a copy of it today
<fuzzy> and it is a huge untapped potential $$
<fuzzy> we have great products…our complaints go down tremendously
<james> I just got off the phone w/bigpipe today
<fuzzy> most of our complaints now are mbout ppl not getting spyware stoppers
<fuzzy> w/ thir stuff
<fuzzy> as opposed to god u guys suck
<fuzzy> so stuff really is changing already
<james> well we have a lot of complaints on the network side against us
<fuzzy> we do actually have sound products…very few chargebacks, etc.
…….
<james> yea, well when firewalls, block our site
<fuzzy> since we advertise so aggressively
<fuzzy> well that's the thing, we advertise so heavily
<fuzzy> we buy more ads than anyone else online
<fuzzy> we’re the biggest clients at most adfirms…
……
<james> its not really the ads
<james> that piss people off
<james> it's the ‘auto-install’
<james> which, I cant care how much people say it doesn't happen, it does
<fuzzy> well like I said, we’re trying to move away from that
<james> somehow, somewhere. :)
<fuzzy> well if you don't exit, yes it does happen
<fuzzy> its not”auto” tho
<fuzzy> and if you don’t know how to get out of it yah it does occur
<james> well if it downloads + executes
<james> heh, its auto installing
<fuzzy> yeah I mean if u click yes
<fuzzy> instead of no
<fuzzy> it downloads
<james> no no
<james> somehow its AUTO installing
<james> no yes/no -> download
<fuzzy> nothing we have auto downloads

<fuzzy> that I am aware of
<fuzzy> and if you find an ad, we need to know of it
<fuzzy> cause we aren't supposed to have it
<fuzzy> everything we have is under ed2…which is yes/no
<fuzzy> and then another warning when they download, telling them they download
<fuzzy> I know, I assure u, of absolutely nothing else marc or Conrad used
<fuzzy> that does otherwise

213. Kristy Ross had daily direct contact with MyGeek account manager, Geoff Gieron. Gieron Depo., Vol. VIII, Ex. 87, p. 9 (31:4 - 31:19), 13 (45:14 - 45:18).

RESPONSE: The sections of Mr. Gieron's deposition that are cited do not support MF #213. Mr. Gieron testified merely that Globedat was an advertiser in the MyGeek system and that he, Gieron, dealt with and worked directly with Globedat representative Kristy Ross who set up the original advertising accounts. (Gieron Depo., Vol. VIII, Ex. 87, p. 9, 31:4-31:19; 13, 45:14-18.) Nowhere is there the statement that Gieron had daily contact with Ross.

214. When MyGeek had problems with the Defendants' advertisements, Gieron contacted Ms. Ross directly to fix any issues. Gieron Depo., Vol. VIII, Ex. 87, p. 21 (79:1 - 79:10), 28 (105:3 - 105:13), 32 (121:6 - 121:18).

RESPONSE: MF #214 misconstrues the testimony. While it is accurate to state that Mr. Gieron contacted Ms. Ross directly to fix issues with the ads, it is not accurate to state as the FTC does that the ads at issue were "defendants' ads". There is no evidence that the ads Kristy Ross placed at MyGeek.AdOn are the same ads or same types of ads as those that were the subject of the FTC Complaint.

215. Gieron had to contact Ms. Ross to fix issues over and over again as publishers and other ad networks constantly complained about the Defendants' advertisements - particularly the way in which the advertisements were delivered. *See e.g.*, Gieron Depo., Vol. VIII, Ex. 87, p. 21 (79:1 - 79:10), 24 (89:4 - 89:20), 28 (105:3 -105:13), 32 (121:6 - 121:18).

RESPONSE: MF #215 misstates the evidence. During the course of the Gieron deposition, the FTC and the defense discussed 17 instances in which either an AdOn traffic partner or someone internally at AdOn complained about the appearance of an ad that was either

identified as having run in one of Ms. Ross' accounts or was suspected to have been an ad run by Ms. Ross. (*See* Group Exhibit, RDX 21, FTC 9, FTC 10, FTC 11, FTC 12, FTC 13, FTC 14, FTC 15, FTC 16, FTC 18, FTC 20, FTC 21, FTC 22-23, FTC 25, FTC 26, KRG23, KRG25.5, and KRG30.) Compared to the magnitude of the impressions of ads that were run during the course of Ms. Ross' business relationship with MyGeek/AdOn, the number does not indicate that complaints were "constant." Far from it. Exhibit 3 to Mr. Gieron's deposition Ex. 87, p. 84-85 lists the total number of impressions per account Ms. Ross maintained at AdOn. If you were to add the far right column of the total number of impressions for each account, this would yield the number of total impressions of ads in all of the accounts maintained by Ms. Ross. This number is in the hundreds of millions. (*See* Gieron Depo., RDX 1, pp. 378:14-25; 379:1-10.) There were 17 documented complaints on approximately 680 million impressions which work out to 1 complaint per 40 million impressions. Furthermore, the complaints were about how the ads appeared not how they were "delivered" apart from the instance discussed in KRG 6. (*See* RDX 22.)

216. In order to resolve complaints, the publishers would send MyGeek screenshots of how the advertisements appeared on their website to consumers. *See, e.g.*, Gieron Depo., Vol. VIII, Ex. 87, p. 22 (84:3 - 85:12); 33 (125:4 - 126:16).

217. MyGeek would forward screenshots they received from their publishers described in MF # 216 to Kristy Ross and ask her to fix the problems. *See, e.g.*, Gieron Depo., Vol. VIII, Ex. 87, p.23 (88:13 - 88:23); 24 (89:4 - 89:20); 32 (121:6 - 121:18); 33 (125:4 - 126:16).

218. MyGeek showed Ms. Ross a DriveCleaner advertisement that contains a pop up window and asked her about it. Gieron Depo., Vol. VIII, Ex. 87, p. 36 (138:11 - 138:25); Ex. 23 to Gieron Depo., Vol. VIII, Ex. 87, pp. 318-319.

219. Ms. Ross responded to seeing the DriveCleaner advertisement discussed in MF # 218 by saying, "This is not a popup, it is flash in the website...this is an example of the scanner...This is certainly not a popup or Active x." Gieron Depo., Vol. VIII, Ex. 87, p. 36 (140:1 - 140:18); Ex. 23 to Gieron Depo., Vol. VIII, Ex. 87, pp. 318-319.

220. The Defendants made more than 70 million dollars by the time they sued each other in Canada over IMI's profits in 2007. Ex. A. to Jain Affid., Vol. X, Ex. 96, p. 14.

RESPONSE: There is no evidence about Ms. Ross obtaining any portion of that $70 million. Indeed, when Messrs. Jain and D'Souza filed suit in Canada seeking to force Marc D'Souza to return $48 million he allegedly stole from IMI, Ms. Ross was not party to that suit, nor is there any evidence that she received any of that money.

221. Marc D'Souza, Sam Jain and Daniel Sundin aired many of their deceptive business practices and outright admitted to the fraud they were committing on consumers in their Canadian pleadings. See, e.g., D.E. #3 (Ex. 17, Att. B) D'Souza Counterclaim, pp. 66-129; Jain Aff., Vol. IX, Ex. 95; Sundin Affid., Vol. VIII, Ex. 89.

RESPONSE: The FTC fails to cite to which sections in this volume of evidence it contends support MF #221. However, none of this evidence implicates Ms. Ross in any deceptive conduct, and in fact, Ms. Ross was not a party to the referenced litigation. Moreover, this unreliable hearsay that should not be used against Ms. Ross in this litigation. The D'Souza Counterclaim is not even signed or verified by Mr. D'Souza.

222. Marc D'Souza, in his counterclaim to the lawsuit brought by his cohorts Daniel Sundin and Sam Jain, admits IMI marketed its computer security software products by using aggressive and misleading pop up advertisements to harass users to purchase their products. D.E. #3 (Ex. 17, Att. B) D'Souza Counterclaim, p. 95, ¶103.

RESPONSE: MF #222 asserts that Marc D'Souza, in the Canadian lawsuit in which Ms. Ross was not a party, "admitted" that IMI "marketed its computer software products using aggressive and misleading pop up advertisements to harass users to purchase their products." The statement in Mr. D'Souza's unsigned and unverified Counterclaim, p. 95, ¶103 was that "[i]n 2003, the Business began to expand its aggressive and in some instances misleading advertising to sell its security software products." Not only does the statement in Mr. D'Souza's affidavit fail to support the FTC's assertion, but the evidence does not identify or relate to Ms.

Ross. Moreover, this statement is unreliable hearsay that should not be used against Ms. Ross in this litigation.

> 223. Sam Jain told D'Souza that IMI could be selling a "block of ice" to paranoid customers with the offer of a cure for computer viruses and still get sales. D.E. #3 (Ex. 17, Att. B) D'Souza Counterclaim, p. 94, ¶101.

RESPONSE: MF #223 involves a statement that Sam Jain allegedly made to Marc D'Souza, based on one of D'Souza's allegations in his unsigned, unverified Counterclaim. Given that Marc D'Souza was sanctioned by the Canadian Court for making false statements in filings, the FTC's reliance on this hearsay is without merit.

224. [IMI's] offshore presence allowed it to escape regulation from the Federal Trade Commission and avoid State Attorneys who were sanctioning and shutting down similar organizations, as well as other civil liabilities from tens of thousands of dissatisfied end consumers. D.E. #3 (Ex. 17, Att. B) D'Souza Counterclaim, p. 102-103, ¶125.

RESPONSE: MF #224 is a statement contained as one of D'Souza's allegations in his unsigned, unverified Counterclaim. Given that Marc D'Souza was sanctioned by the Canadian Court for making false statements in filings, the FTC's reliance on this hearsay is without merit.

> 225. Daniel Sundin, in his affidavit submitted February 19, 2007, attached a copy of the exact same "948 dangerous files" DriveCleaner advertisement that the FTC's Investigator saw at least eight times, is discussed in the IMI chat logs, and that Kristy Ross confirmed as IMI's DriveCleaner advertisement to MyGeek. Ex. D to Sundin Affid., Vol. VIII, Ex. 89, p. 465; D.E. #3 (Ex. 20), Drexler Decl., p. 66, ¶197; MF ## 205, 218-219; Novick Decl., Vol. XII, Ex. 103, pp. 15-16, ¶6.

RESPONSE: MF #225 is false and is contradicted by Ms. Novick's own Declaration. Novick Decl., Vol. XII, Ex. 103, pp. 15-16, ¶6. While the FTC claims that Ms. Novick saw this advertisement at least ***eight*** times, in Paragraph 6, Ms. Novick declares "On at least ***one*** of these occasions, the advertisement I reviewed was identical to the advertisement Daniel Sundin included in his Affidavit. . . ." Furthermore, the ad Ms. Ross discussed with Mr. Gieron was

not the ad Ms. Ross submitted or the ad that ran on the AdOn network because Ms. Greenberg tested the wrong link. *See* Response to MF # 61 above.

226. Marc D'Souza and Kristy Ross have asserted their Fifth Amendment privilege against self-incrimination throughout the litigation of this case. Kristy Depo., Vol. VII, Ex. 65, pp. 1-73; D'Souza Depo., Vol. VII, Ex. 66, pp. 74-150.

RESPONSE: The FTC's reference to certain defendants' individual decision to assert their Fifth Amendment rights is inappropriate because the Court previously stated that "I will say it's almost a given that the government is not going to be able to introduce evidence of the assertion of a Fifth Amendment privilege in this case." (June 9, 2009-Hearing, RDX 23, p. 52:24-25; 53:1.) Thus, the FTC's attempt to introduce such evidence is inapt.

227. Marc D'Souza admitted to a Canadian Court, through his counterclaim and affidavits, that he and the other Defendants purposefully misled consumers into purchasing their computer security products through deceptive and aggressive advertising. MF #222; D'Souza Affid., Vol. 10, Ex. 97, p. 59, ¶56, p. 65, ¶85, p. 68, ¶¶96-97.

RESPONSE: MF # 227 cites to the same incorrect recitation of a claim by D'Souza that is discussed in Response to MF # 222 above. This allegation further cites to D'Souza Affid., Vol. 10, Ex. 97, p. 59, ¶56 for the claim that "Defendants" misled consumers. Significantly, this paragraph of D'Souza's affidavit refers to "Jain" and "Sundin" being "aware of the sophisticated network of corporate entities and offshore bank accounts held by the D'Souzas." Far from implicating defendant Ross, this recitation exonerates her. The citations to D'Souza Affid., p. 65, ¶85 have nothing to do with misleading customers but to a trust set up by the D'Souzas to protect against liabilities from disgruntled customers and p. 68, ¶¶ 96-97 involve specifics of a dispute between D'Souza and Sundin involving the allegation of forgery by D'Souza. The evidence does not relate to Ms. Ross. Further, given that Marc D'Souza was sanctioned by the Canadian Court for making false statements in filings, the FTC's reliance on this hearsay is without merit.

228. When confronted about his admissions at deposition, Marc D'Souza refused to respond, citing the Fifth Amendment. D'Souza Depo., Vol. VII, Ex. 66, pp. 74-150.

RESPONSE: *See* Response to MF # 226.

229. Kristy Ross admitted to representatives at MyGeek that the Defendants' scanner ads are nothing more than Flash animations. MF ## 218-219.

RESPONSE: MF # 229 misstates the evidence. *First*, Ms. Ross' comments about the ads contained at D.E. #186-3, Gieron Depo. Ex., Vol. VIII, Ex. 87, pp. 318-319 are restricted to this particular ad not to any other ad run by Ms. Ross or anyone else at IMI. *Second*, Ms. Ross' exact statement is important. Ms. Ross does not state that the ads are in the format of flash ads or flash banner ads but merely states that a box in the DriveCleaner ad is "a flash in the website" and "an example of the scanner." (Gieron Depo., pp. 140:1-140:18.) When questioned about the ads appearing at Vol. VIII, Ex. 87, pp. 318-319, KRG 27, RDX 5, p20-21, Mr. Gieron explains that flash ads are creative formatting within a web page. (Gieron Depo., RDX 1, p. 342:10-16.) This type of formatting consists of images that can change. (Gieron Depo., RDX 1, p. 342: 24.) Mr. Gieron states; "Flash is not 100% safe. It has the capability of changing whenever. That's all controlled by the creator of the flash file." (Gieron Depo., RDX 1, p. 343: 11-13.) Gieron was also not able to pin down exactly how the ad under discussion here actually operated. Gieron stated; "I only know what I – what I see here and from memory is similar to what I saw there. What other functionality it was able to provide, I couldn't tell you." (Gieron Depo., RDX 1, p. 349:14-17.) In light of the variability of flash ads themselves and the ambiguity in Ms. Ross' statement that she saw a "flash in the website" it is not possible to conclude that the statement is an admission about the behavior or this ad, much less that of ads run by "Defendants."

230. Ross submitted numerous ads to MyGeek that contained the Defendants' fake system scans. MF # 52.

RESPONSE: MF # 230 is false. MF # 230 simply cites to MF #52. Neither MF # 230, nor MF # 52 is supported by the referenced exhibits. While, MF # 230 refers to "Defendants" without differentiation, none of the exhibits establish that Kristy Ross "created" advertisements that appeared to scan customers' computers. The exhibits listed from the Gieron deposition are FTC 13, RDX 15; FTC 14, RDX 24; FTC 15, RDX 25; FTC 20, RDX 26 and FTC 23, RDX 27. *See* Response to MF # 166 above which contains a specific discussion of each of the exhibits cited by the FTC and the limitations in the FTC's ability to link the ads themselves to Ms. Ross. In addition, there is no evidence that these ads contain fake system scans. In fact, the evidence is to the contrary. With respect to FTC 13, RDX 15; FTC 14, RDX 24, and FTC 15, RDX 25, Mr. Gieron testified that based on the wording of the ads, his assumption would be that the ad was not purporting to scan the computer. (Gieron depo., RDX 1, p. 419: 17-21.) With respect to FTC 20, RDX 26, Mr. Gieron testified that the dialog boxes contained in the ad do not purport to scan the consumer's computer. (Gieron Depo., RDX 1, p. 430:16-23.) The ad discussed at FTC 23, RDX 27, is the subject of the Response to MF # 229 above. *See also* Response to MF # 61 above for a discussion of ads placed by Ms. Ross.

231. Ross opened 54 MyGeek accounts which she used to submit IMI ads that were displayed over the MyGeek network. MF # 65.

RESPONSE: *See* Response to MF # 65 above.

232. Ross paid for some IMI ads displayed through MyGeek with her own credit card. Ballapragada Decl., Vol. VIII, Ex. 88, p. 448; MF # 351.

233. Marc D'Souza's and Daniel Sundin's credit cards were also used to pay for IMI ads displayed through MyGeek. MF # 31.

RESPONSE: *See* Response to MF # 31 above.

234. Ross was MyGeek's sole contact for IMI. MF # 213, Gieron Depo., Vol. VIII, Ex. 87, p. 13 (45:14-18); 51 (200:15-22).

RESPONSE: MF # 234 misstates the evidence. Mr. Gieron never testified that Ms. Ross was My Geek's sole contact. Indeed, he testified that from time to time he worked with other persons. Specifically, and among other things, Mr. Gieron testified:

> Q: So you associate [certain numbered accounts] with Kristy because she was sort of the face that you had when you had when you were dealing with the accounts?
> A: Right.
> Q: But as you look at the accounts, do you know whether or not there was somebody else besides Kristy Ross who was accessing these accounts?
> A: I do not .

(Gieron Depo., RDX 1, p. 185: 3-10.) *See also* Response to MF ## 212-214 above.

235. When the FTC asked Ross about the fake scan ads at deposition, she asserted her Fifth Amendment rights rather than answer the FTC's questions. Ross Depo., Vol. VII, Ex. 65, pp. 1-73.

RESPONSE: *See* Response to MF # 226.

236. D'Souza and Ross invoked the Fifth Amendment hundreds of times in response to every substantive question posed by the FTC. Ross Depo., Vol. VII, Ex. 65, pp. 1-73; D'Souza Depo., Vol. VII, Ex. 66, pp. 74-150.

RESPONSE: *See* Response to MF # 226.

237. In 27 of the sworn consumer declarations submitted by the FTC, consumers describe their experiences with the defendants' software. Hurd Decl., Vol. I, Ex. 22, pp. 44-46; Fieler Decl., Vol. I, Ex 12, pp. 26-27; Oswald Decl., Vol. I, Ex. 35, pp. 68-69; Golden Decl., Vol. I, Ex. 16, pp. 33 - 34; Foster Decl., Vol I, Ex. 14, p. 29; Welander Decl., Vol. I, Ex. 50, pp. 93-94; Martin Decl., Vol. I, Ex. 31, pp. 62-63; Myers Decl., Vol I, Ex. 33, p. 66; Church Decl., Vol. I, Ex. 6, pp. 13-14; White Decl., Vol. I, Ex. 51, pp. 95-96; Stalvey Decl., Vol. I, Ex. 46, pp. 86-87; Ruszkowski Decl., Vol. I, Ex. 44, pp. 83-84; Harris Decl., Vol. I, Ex. 18, pp. 36-37; Hildebrand Decl., Vol. I, Ex. 19, pp. 38-39; Furney Decl., Vol. I, Ex. 15, pp. 30-31; Hunt Decl., Vol. I, Ex. 21, p. 43; Pritchett Decl., Vol. I, Ex. 39, pp. 74-75; Cherup Decl., Vol. I, Ex. 5, p. 12; Baker Decl., Vol. I, Ex. 3, p. 10; Hodge Decl., Vol. I, Ex. 20, p. 41-42; Cucura Decl., Vol. I, Ex. 7, pp. 16-17; Small Decl., Vol. I, Ex. 45, p. 85; Liotta Decl., Vol. I, Ex. 28, p. 56; Layton Decl., Vol. I, Ex. 26, pp. 52-53; Thompson Decl., Vol. I, Ex. 48, pp. 89-90; Marcynzsyn Decl., Vol. I, Ex. 30, pp. 59-61; Roberts Decl., Vol. I, Ex. 43, pp. 81-82.

RESPONSE: Of the 27 consumers referenced in MF # 237, a review of each declaration reveals that at least 21 of them complained about software that the FTC's investigator admits

Kristy Ross had nothing to do with. (FTC Vol. XII, Ex. 103, Attachment A, pp. 28-30, Drexler Dec., ¶ 110.) Moreover, these declarations are hearsay.

238. These consumer declarations paint a clear picture of shoddy software sold to consumers who were duped into purchasing the defendants' products. MF #237.

RESPONSE: MF #238 states that the consumer complaints evidence shoddy software sold to consumers who were "duped into buying defendants' products." None of the customer declarations cited in support of this assertion establishes that the software that was sold was defendant Ross' software or even that ads that might be able to be identified to Ms. Ross were the ads to which these disgruntled consumers responded when and if they made software purchases. *See* Response to MF # 237.

239. Many of the consumer declarants report that the Defendants' software either failed entirely to function or actually damaged their computers. *See, e.g.*, Fieler Decl., Vol. I, Ex 12, pp. 26-27; Furney Decl., Vol. I, Ex. 15, pp. 30-31; Hildebrand Decl., Vol. I, Ex. 19, pp. 38-39; Pritchett Decl., Vol. I, Ex. 39, pp. 74-75.

RESPONSE: MF #239 refers to "defendants' software." However there is no evidence cited that establishes that Ms. Ross developed or created the software. These consumer declarations are hearsay and should be excluded under Fed. R. Evid. 802.

240. Consumers also consistently report that the Defendants were impossible to reach, and that refund demands were met with absolutely no response. *See, e.g.*, Harris Decl., Vol. I, Ex. 18, pp. 36-37, ¶7; Church Decl., Vol. I, Ex. 6, pp. 13-14 ¶7; Hurd Decl., Vol. I, Ex. 22, pp. 44-46, ¶10; Welander Decl., Vol. I, Ex. 50, pp. 93-94, ¶4; Cucura Decl., Vol. I, Ex. 7, pp. 16-17, ¶5.

RESPONSE: MF #240 states that "Defendants were impossible to reach." There is no evidence that Ms. Ross was ever employed in any capacity such that part of her job description was to respond to customer complaints. In fact her employment description of "business expansion, sales and marketing, and product optimization." (D.E. #186-3, Ross Affid., Vol. I, Ex. 2, p.7, ¶1 ("Ross Affid").) would, by its terms, have nothing to do with responding to

customer complaints. *See* Response to MF # 239.

241. Consumers report that the Defendants' software displays trademarks belonging to the Microsoft Corporation including a replica of the Microsoft Windows Security Shield logo. Welander Decl., Vol. I, Ex. 50, pp. 93-94, ¶2; Marcynzsyn Decl., Vol. I, Ex. 30, pp. 59-61, ¶3; Hodge Decl., Vol. I, Ex. 20, pp. 41-42, ¶3; Cucura Decl., Vol. I, Ex. 7, pp. 16-17, ¶2; Furney Decl., Vol. I, Ex. 15, pp. 30-31, ¶3.

RESPONSE: MF #241 refers to "Defendants' software." But there is no support for the assertion that the software that was the subject of the listed complaints was created or developed by defendant Ross. *See* Response to MF # 239.

242. Consumers report that by using Microsoft's trademarks as described in MF # 241, the Defendants led numerous consumers to believe that the Defendants' products are affiliated with Microsoft. Welander Decl., Vol. I, Ex. 50, pp. 93-94, ¶2; Marcynzsyn Decl., Vol. I, Ex. 30, pp. 59-61, ¶3, Hodge Decl., Vol. I, Ex. 20, pp. 41-42, ¶3; Cucura Decl., Vol. I, Ex. 7, pp.16-17, ¶2; Furney Decl., Vol. I, Ex. 15, pp. 30-31, ¶3.

RESPONSE: MF #242 refers to actions of "Defendants" generally. There is no support that the software that was the subject of the listed complaints was created or developed by defendant Ross or that she placed any of the ads to which they responded. *See* Response to MF # 239.

243. Consumers report that the Defendants used the name "Windows" or "Win" in their product names which caused confusion because some consumers believed the product was from Microsoft. Baker Decl., Vol. I, Ex. 3, p. 10 (Windows AntiVirus); Hodge Decl., Vol. I, Ex. 20, pp. 41-42, ¶3 (WinSpywareProtect); Martin Decl., Vol. I, Ex. 31, pp. 62-63 (WinXProtector); Marcynzsyn Decl., Vol. I, Ex. 30, pp. 59-61 (WinAntivirus Pro); Kilby Decl., Vol. I, Ex. 24, p. 49 (WinFixer).

RESPONSE: MF #243 states that "Defendants used" Windows based names causing confusion. There is no evidence to support the assertion that Ms. Ross had any role in naming any IMI product. *See* Response to MF # 239.

244. Consumers report that the Defendants' software was forced onto their computers without their consent. Small Decl., Vol. I, Ex. 45, p. 85; Roberts Decl., Vol. I, Ex. 43, pp. 81-82.

RESPONSE: MF #244 refers to "Defendants' software." There is no evidence that Ms.

Ross created or developed any of the software sold to consumers. *See* Response to MF # 239.

245. Consumer Sally Small was on the official website for the National Association of Realtors when she was involuntarily redirected to the Defendants' *drivecleaner.com* website. Small Decl., Vol. I, Ex. 45, p. 85, ¶¶2-3.

RESPONSE: MF #245 refers to "Defendants' drivecleaner.com website". There is no evidence of any connection between Ms. Ross and the drivecleaner.com website. The site was not set up or registered to Ms. Ross and there is no evidence that she controlled any of its content. *See* Response to MF # 239.

246. The DriveCleaner website informed Small that her computer might contain pornographic material and that she should download DriveCleaner to check her computer for such files. Small Decl., Vol. I, Ex. 45, p. 85, ¶¶2-3.

RESPONSE: *See* Response to MF # 239.

247. Despite clicking "no" and "cancel" on the DriveCleaner website, the DriveCleaner software was forcibly downloaded to Small's computer. Small Decl., Vol. I, Ex. 45, p. 85, ¶3.

RESPONSE: *See* Response to MF # 239.

248. Small had installed Norton Antivirus on her computer which detected DriveCleaner as a threat and removed the product from her computer. Small Decl., Vol. I, Ex. 45, p. 85, ¶¶2-3.

RESPONSE: *See* Response to MF # 239.

249. FTC computer expert Kevin Johnson tested a number of software products sold by the Defendants, including WinAntiVirus 2005, ErrorPatrol, PerformanceOptimizer, AntiMalwareGuard, ErrorClean, AntiVirusXP2008, PCTurboPro, ErrorSafe and WinFixer. Expert Report of Kevin Johnson, Vol. VI, Ex. 63, pp. 496-498; Rebuttal Report of Kevin Johnson, Vol. VI, Ex. 64, pp. 512-523; Novick Decl., Vol. XII, Ex. 103, pp. 13-15, ¶4; MF ## 352-360; 363-364.

RESPONSE: MF #249 refers to software products sold by the "Defendants.'" There is no evidence that defendant Kristy Ross sold any of these products except WinAntiVirus2005 and Errorsafe. The facts are to the contrary. (D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30; Drexler Dec., ¶ 110.)

250. In each and every case, Mr. Johnson found the Defendants' software makes false and misleading representations "designed to scare a user into purchasing the scanning software." Expert Report of Kevin Johnson, Vol. VI, Ex. 63, pp. 496-498; Rebuttal Report of Kevin Johnson, Vol. VI, Ex. 64, pp. 512-523.

RESPONSE: MF # 250 incorrectly assumes that Mr. Johnson's opinion is an undisputed fact. Mr. Johnson's opinion, which was contradicted by Mr. Ellis, is not a fact, but instead, simply Mr. Johnson's opinion.

251. Johnson found that the Defendants' PCTurboPro product used "scare tactics to convince users they need to purchase the registered version," including wildly misrepresenting the amount of space left on the hard drive of the "scanned" computer and falsely warning users that their computers were in a "CPU Overload" state. Rebuttal Report of Kevin Johnson, Vol. VI, Ex. 64, pp. 520-522.

RESPONSE: MF #251 refers to "Defendants' PC TurboPro program." There is no evidence that defendant Kristy Ross developed any software product and no evidence that she sold the PCTurboPro program. The facts are to the contrary. (D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30; Drexler Dec., ¶ 110.)

252. The Defendants' PCTurboPro program warned users that "running programs may freeze and you loose all data" [*sic*] and instructed users that "you must have a registered version of PCTurboPro to get rid of the problems." Rebuttal Report of Kevin Johnson, Vol. VI, Ex. 64, pp. 520-522.

RESPONSE: *See* Response to MF # 251 above.

253. Daniel Kim, the expert retained by Marc D'Souza, conceded that he witnessed PCTurboPro making the same false representations Mr. Johnson observed. Kim Depo., Vol. VII, Ex. 86, pp. 479-480 (252:18 - 256:25).

RESPONSE: *See* Response to MF # 251 above.

254. Mr. Kim stated that he did not agree with PCTurboPro's findings. Kim Depo., Vol. VII, Ex. 86, pp. 479-480 (252:18 - 256:25).

RESPONSE: *See* Response to MF # 251 above.

255. Ms. Ross's expert, Scott Ellis, stated that he did not conduct any testing of PCTurboPro because PCTurboPro was not on the list of programs Ms. Ross's counsel authorized him to test. Ellis Depo., Vol. VI, Ex. 62, p. 331 (138:6 - 138:12).

RESPONSE: The FTC's implication in MF # 255 that Ms. Ross's counsel somehow tried to tie Mr. Ellis's hands in that Ms. Ross's counsel only "authorized" Mr. Ellis to test certain products is baseless. Mr. Ellis testified to the same:

> Q: But you won't test these files unless Ms. Gurland lets you.
> A: Its not a matter of her letting me. I'm a retained expert, and if I felt there was a need to test them, I would test them, and that's certainly a discussion that we may have.

(Ellis Depo., RDX 28, p. 140:19-24.) Later in Mr. Ellis' deposition, when FTC counsel returns to the same point, Mr. Ellis testifies as follows:

> Q: Were there files that you asked to test that Ms. Gurland said no?
> A: No. No.

(Ellis Depo., RDX 28, p. 164:9-11.) When defense counsel was able to conduct follow-up with Mr. Ellis on his testing selections, the following exchange took place:

> Q: Now that there is an MD5 hash, is there any – has there ever been any conversation between you and counsel that indicated that they wouldn't want the free products of those tested?
> A: No. I don't recall anyone saying don't do that, no.
> Q: Okay. And indeed with respect to any of the products, there was no direction to tell you what to do; is that right? That you couldn't do something?
> A: Right.
> Q: Because – and just to be clear, if counsel would have told you, here's a hard drive, and I'm instructing you you may not run those tests, would you have agreed to the engagement?
> A: Probably not.

(Ellis Depo., RDX 28, pp. 301:22-25-302:1-11.)

The FTC's suggestion is ironic in that FTC expert Kevin Johnson testified that it was the FTC who directed him which files to look at and which files to test. (Johnson Depo., RDX 29, pp. 27:7-22-20; 68:11-21-69:1-16.) Indeed, with respect to the 6 binaries Johnson tested, he was not given nor did he ask for the FTC's rationale. Johnson testified;

> Q: How did you select the six binaries that you ran?
> A: I believe there were five or six. They were the ones I was provided.
> Q: And were you given any rationale about why these and not others?

A: No.
Q: Do you know how many binaries were on that hard drive?
A: Not off the top of my head.

(Johnson Depo., RDX 29, p. 89:1-10.)

256. ErrorPatrol is one of the Defendants' software products that purports to detect "Severe System Threats" on consumers' computers. Expert Report of Kevin Johnson, Vol. VI, Ex. 63, p. 497; Rebuttal Report of Kevin Johnson, Vol. VI, Ex. 64, pp. 514-516; Novick Decl., Vol. XII, Ex. 103, pp. 19-21, ¶¶15-22**.**

257. Mr. Johnson tested ErrorPatrol on a pristine computer that had never been connected to the Internet and contained only the files installed by default by Microsoft Windows XP. On this "out of the box" machine, ErrorPatrol found "318 Severe System Errors" that were "very likely to create further problems" including such ominous developments as "lost documents," "physical data loss," "system not starting up," and "system slowdowns, crashes and freezes." Rebuttal Report of Kevin Johnson, Vol. VI, Ex. 64, p. 515.

258. Mr. Johnson states in his report that ErrorPatrol detects core components of Microsoft Windows XP that exist in every copy of the operating system as "Severe System Threats," and concludes that it would be "impossible" for these core Windows components to "cause any of the events warned about by this software." Rebuttal Report of Kevin Johnson, Vol. VI, Ex. 64, p. 516.

RESPONSE: MF # 250 incorrectly assumes that Mr. Johnson's opinion is an undisputed fact. Mr. Johnson's opinion, which was contradicted by Mr. Ellis, is not a fact, but instead, simply Mr. Johnson's opinion. *See* Response to MF # 259 below.

259. Mr. Kim and Mr. Ellis, the Defendants' experts, were essentially in agreement with Johnson's analysis as described in MF # 258. MF ## 260-265.

RESPONSE: MF #259 is false. MF # 258 states that FTC expert Kevin Johnson's conclusion about Errorpatrol was: (1) "that ErrorPatrol detects core components of Microsoft Windows XP that exist in every copy of the operating System as "Severe System Threats" and (2) that it "would be 'impossible' for these core Windows components to 'cause any of the events warned about by this software." (D.E. #186-3, Rebuttal report of Kevin Johnson, Vol. VI, Ex. 64, p. 516.) With respect to the first assertion, Mr. Ellis did not testify that Errorpatrol

detects "core components of Microsoft Windows XP." He testified that Errorpatrol detected registry entries that lacked prog IDs that would likely be included in every install of Windows XP. (Ellis Depo., RDX 28, pp. 179: 8-14 181:7-17.) The distinction is important because far from viewing these registry entries as core components of the Microsoft system, Mr. Ellis testified that in his opinion these items were things that should be removed from a consumer's operating system. (Ellis Depo., RDX 28, pp. 186:4-16; 192:7-10; 193:5-7; 193:17-25; 195:1-14; 197:6-9; 200:1-4; 200:7-13.) With respect to the second assertion, Mr. Ellis' testimony was the opposite of what the FTC claims in MF # 259. Mr. Ellis testified on numerous occasions that the items identified by ErrorPatrol as severe system threats were indeed severe system threats. Mr. Ellis testified, for example, that:

> A: I believe if we look at the popup it says – it says they are very likely to. It doesn't say these are definitely causing it. It says they are very likely to create further problems if not fixed.
> Q: Okay. So do you believe that these –
> A: Yeah, I mean, I know there is problems on my computer. If we don't fix them, eventually my computer will crash.

(Ellis Depo., RDX 28, pp. 174: 1-2, 180:17-20, 181:23-25-182:1-8, 182:11-25, 183:1-19, 192:1-5, 193:1-7, 195:1-14, 200:5-13.)

> 260. When asked if the core Windows components that ErrorPatrol detects as "Severe System Threats" could possibly cause the parade of horribles the software claims, Mr. Kim testified "I don't think so." Kim Depo., Vol. VII, Ex. 86, p. 487 (282:18 - 282:25).

> 261. Mr. Kim acknowledged that ErrorPatrol misrepresents the "threats" it detects on consumers' computers:
> Q. Now, to me, that indicates that ErrorPatrol believes that Windows ships from the factory with 318 severe system threats very likely to cause [lost documents and profile settings, physical data loss, system not starting up and system slowdowns, crashes and freezes.] If you disagree with that statement, explain to me why.
> A. Yeah. Again -- yeah, I don't necessarily agree with the assessment of the threat that it's presenting, severe threat.
> * * *
> A. Yeah, I would not -- I do not necessarily agree with the threat level it's

presenting. Kim Depo., Vol. VII, Ex. 86, p. 486 (279:8 - 280:16).

262. Mr. Ellis testified that ErrorPatrol detects files present by default in every install of Windows XP as "Severe System Errors." Ellis Depo., Vol. VI, Ex. 62, p. 352 (181:14 - 181:17; 182:17-182:22, p. 343 (186:17 - 186:25).

263. Mr. Ellis testified that he did not believe that all of the system errors detected by ErrorPatrol were capable of causing the deleterious effects that ErrorPatrol claims. Ellis Depo., Vol. VI, Ex. 62, p. 343 (185:23 - 185:25, 186:1 - 186:3, 186:22 - 186:25).

RESPONSE: MF #263 asserts that Mr. Ellis testified that "he did not believe that all of the system errors detected by ErrorPatrol were capable of causing the deleterious effects that ErrorPatrol claims." (Ellis Depo., RDX 28, pp. 185:23-25, 186:1-3, 186:22-25.) While this was Mr. Ellis initial statement on the matter, he, on the immediately following pages of the deposition, clarified his answer to state that it would depend on the user system. Ultimately, Mr. Ellis testified that he was not sure whether the registry keys inquired about by the FTC were very likely to cause the errors stated in the ErrorPatrol ad. (Ellis Depo., RDX 28, pp. 187:4-25, 188:1-19.)

264. Mr. Ellis testified that he had not removed any of the core Windows components that ErrorPatrol detects as "Severe System Errors" from the computers that he and his wife use. Ellis Depo., Vol. VI, Ex. 62, p. 343 (188:25) p. 344 (189:22).

RESPONSE: The statement contained in MF #264 is inaccurate and misleading. Mr. Ellis actually started to testify that he did not manage his wife's computer and then stated "the shoekeeper's son has no shoes." (Ellis Depo., RDX 28, pp. 188:25-189:1.) Mr. Ellis went on to say that he might have run ErrorPatrol on his wife's computer Ellis Depo., RDX 28, p. 189:7-11, that he did not remove the registry keys at issue from the computer that he used before he gave it to his wife because that was years ago and he did not know about the keys at that time Ellis Depo., RDX 28, p. 189:15-1, and that he was going to remove the particular registry keys from his wife's computer. (Ellis Depo., RDX 28, p. 189:19-23.) Furthermore, Mr. Ellis testified that

in 2006 and 2007 he did not remove the registry keys being discussed from his laptop because he did not then know about them and that at that time he actually did click on a link that compromised his computer. (Ellis Depo., RDX 28, p. 190:12-22.)

> 265. Mr. Ellis, when asked if he agreed with ErrorPatrol's claim that all cookies present on a scanned computer constitute "Severe System Threats," he answered:
> Q. And do you think it is likely that ErrorPatrol would have detected any cookie in the cookie folder as a severe system threat?
> A. Yeah, I think that's how the software operates.
> Q. And in some cases those would actually not be severe system threats.
> A. That would be accurate.

(Ellis Depo., Vol. VI, Ex. 62, p. 34 (212:14 - 212:20).)

RESPONSE: MF # 265 contains a particular interchange with Mr. Ellis about cookies being identified by the ErrorPatrol software as severe system threats. Mr. Ellis, as part of the same section of testimony, confirmed that a cookie could be a severe system threat with the potential to create lost documents and profile settings through an existing exploit. (Ellis Depo., RDX 28, pp. 208:22-24-209:1-12.) Mr. Ellis also made it clear that while ErrorPatrol could not distinguish between different types of cookies, no software would be able to do that other than the software that created the cookie. (Ellis Depo., RDX 28, p. 213:9-15.) Mr. Ellis made it clear that the behavior exhibited by ErrorPatrol in identifying every cookie was standard software behavior, "And that's generally how these software programs work; they say this is a problem, you need to clean it up, even if there is just one cookie or one URL history item in there. They will mention it and say these are problems." (Ellis Depo., RDX 28, p. 216:130-217.) Finally, Mr. Ellis made it clear that the ErrorPatrol software warning that was at issue did not claim that one file would cause a problem but rather alerted in terms of the plurality of all the errors listed. (Ellis Depo., RDX 28, pp. 308:14-19, 309:12-15, 310:6-11.)

> 266. Johnson testified that virtually every computer in the world has cookies stored upon it. Johnson Depo., Vol. VII, Ex. 67, p. 202 (200:19 - 200:22).

267. Kevin Johnson received the similar results with all of the Defendants' products he tested in his report. MF # 250.

268. When Mr. Johnson tested the Defendants' WinFixer program, he found that the program detects core Windows components as "Severe System Threats," and concluded that it would be "impossible" for these Windows components to cause the parade of horribles that WinFixer claims are "very likely" if the components are not removed. Rebuttal Report of Kevin Johnson, Vol. VI, Ex. 64, p. 520.

RESPONSE: MF # 268 incorrectly assumes that Mr. Johnson's opinion is an undisputed fact. Mr. Johnson's opinion, which was contradicted by Mr. Ellis, is not a fact, but instead, simply Mr. Johnson's opinion. *See* Response to MF # 259 above and MF # 269 below.

269. When asked about Mr. Johnson's findings, Mr. Ellis stated that he did not know what the Windows components detected by WinFixer did, but agreed that items WinFixer detected as "severe system threats" would not cause the problems claimed by the program. Ellis Depo., Vol. VI, Ex. 62, p. 358 (246:1 - 246:18, 248:13 - 248:16).

RESPONSE: While admitting that he did not know precisely what the registry keys flagged by Winfixer did, Mr. Ellis was able to state that there was an area of the registry where items use keys to link to other areas of the registry and that software like Winfixer goes through to make sure the chains are complete because incomplete chains with orphan records are not good to have on ones computer. (Ellis Depo., RDX 28, p. 46: 2-10.) On this point, Mr. Ellis was not certain that every copy of Windows XP even has the keys identified by Winfixer because he was not certain that certain VMWare such as was used by both FTC expert Johnson and Ellis for testing, did not install things on the local machine. Counsel for the FTC encouraged Mr. Ellis to undertake the additional tests to see what affect VM Ware had on the registry of the local machine. (Ellis Depo., RDX 28, pp. 246:18-25-247:1-9.) When Mr. Ellis made the statement cited in this MF, he was referring to that 50 or so registry entries of a test that FTC counsel ran on Winfixer. Counsel for Ms. Ross objected to the procedure of FTC counsel asking questions of the witness based on FTC's counsel's own testing. (Ellis Depo., RDX 28, p. 242:13-16.) Mr.

Ellis qualified his statement that the particular items identified by Winfixer would not yet cause a problem by stating that they would contribute to a problem over time, (Ellis Depo., RDX 28, p. 248:14-16) by stating that the 50 or so entries were akin to a slap in the face and Winfixer's warning was akin to saying "let's "get rid of it, stop it from happening, let's clean it up," Ellis Depo., RDX 28, p. 249:1-2, by stating that the files identified were "one of the straws on the came's back," Ellis Depo., RDX 28, p. 249:3-4, and ultimately by stating that he did not know that the files identified by Winfixer were or were not severe system threats Ellis Depo., RDX 28, pp. 250:25-251:1-3 stating; "I don't want to tell you that these—that these are not all straws on the camels back because they might be. If there is, in fact, a problem with a driver or something like that and that's why these didn't get installed, I wouldn't know." (Ellis Depo., RDX 28, p. 250:20-24.)

> 270. FTC Investigator Novick tested the Defendants' WinFixer software and found that WinFixer detects any and all cookies stored on the computer as "Severe System Threats" that are "very likely to create further problems if not fixed immediately, such as: lost documents and profile settings, physical data loss, system not starting up, system slowdowns, crashes and freezes." Novick Decl., Vol. XII, Ex. 103, pp. 17-19, ¶¶11-14.
>
> 271. These text files are present on virtually every computer that accesses the Internet, and are incapable of causing any of the dire results warned of by the WinFixer software. Johnson Depo., Vol VII, Ex. 67, p. 202 (200:13 - 200:22); Johnson Rebuttal Report, Vol. VI, Ex. 64, pp. 519-520.

RESPONSE: The Johnson deposition supports the assertion that Johnson estimates that text files in the form of cookies are present on 99% of computers. The sections of the Johnson report cited do not relate to text files as stated in the MF but to Winfixer's identification of registry keys as severe system threats. Moreover, Johnson's assertion that Winfixer misidentifies files is not a fact in the case. It is Johnson's conclusion as to which there is a significant factual dispute between the experts. (Ellis Depo., RDX 28, pp. 243:23-25; 244:1-4; 245:5-9; 208:10-25;

209:1-12; 209:13-25; 210:23-25; 211:1-9; 211:17-25; 212:1-5; 213:6-15; 215:11-25; 216:1-22; 217:9-16.) Specifically, Mr. Ellis testified as follows:

> Q: And while I understand your personal preference, would you say that a cookie is a severe system threat?
> A: I would say it could be.
> Q: Would you say that a cookie is very likely to create lost documents and profile settings?
> A: The potential is there.
> Q: And how would that be?
> A: Through an exploit that existed. I believe in 2006, 2005, around that time, there was an exploit that would allow anybody to read any cookie at all that was on your system, which cookies contain passwords and stuff like that. So yeah, it was definitely something that all software was wanting to—any security software at all would scrub cookies from your system if you wanted to keep it clean."

(Ellis Depo., RDX 28, pp. 208:22-25; 209:1-12.)

272. The WinFixer program itself creates a cookie when first installed, and then proceeds to detect the very cookie it created as a "Severe System Threat." Novick Decl., Vol. XII, Ex. 103, p. 12, ¶18.

273. Defense expert Ellis thought the conduct described in MF # 272 was "troublesome." Ellis Depo., Vol. VI, Ex. 62, p. 357 (244:21 - 244:25).

RESPONSE: This assertion is misleading. MF #273 does not disclose that the exhibit about which FTC counsel was questioning Mr. Ellis over defense counsel's objection was Exhibit 10 which was prepared by FTC counsel and was not the subject of Mr. Johnson's report or Mr. Ellis' testing. (Ellis Depo., RDX 28, pp. 242:13-16.) Before making the statement that the behavior shown on FTC counsel's testing exhibit was "troublesome," Mr. Ellis stated that he did not see this behavior in his own testing and that he was not able to speak to the reasons for this behavior without doing his own analysis. (Ellis Depo., RDX 28, pp. 243:23; 244:11-16.) Mr. Ellis' Supplemental Report tests the free version of Winfixer and concludes that its functionality was not in alignment with malicious adware products. (Ellis Supplemental Report, RDX 30, p. 2.)

274. FTC Investigator Novick tested the Defendants' Winfixer software and found that WinFixer detects any text file within the Window's Cookie directory as a "Severe System Threat," even text files that contain no data. Novick Decl., Vol. XII, Ex. 103, pp. 17-19, ¶¶11-14.

275. ErrorPatrol detects both cookies and Internet browser history as "Severe System Threats," that are "very likely to create further problems if not fixed immediately, such as: lost documents and profile settings, physical data loss, system not starting up, system slowdowns, crashes and freezes." Novick Decl., Vol. XII, Ex. 103, pp. 19-20, ¶¶15-18.

276. FTC testing found that ErrorPatrol detects all website visits as a "Severe System Threat," including a visit to *www.mdd.uscourts.gov*, the official website for this Court. Novick Decl., Vol. XII, Ex. 103, p. 20, ¶17.

277. FTC testing found that ErrorPatrol detects any text file within the Windows Cookies directory as a threat, regardless of its content. Novick Decl., Vol. XII, Ex. 103, p.19-20, ¶¶15-16.

278. When the FTC tested AntiMalwareGuard the program "detected" 23 different malicious programs on a pristine computer that had never been connected to the Internet and did not contain any malicious software. Novick Decl., Vol. XII, Ex. 103, pp. 22-23, ¶26.

279. FTC testing confirmed Kevin Johnson's findings that Defendants' PCTurboPro, ErrorClean, AntiVirus XP 2008, PerformanceOptimizer, and WinAntiVirus products issue false and misleading warnings to consumers for the sole purpose of frightening consumers into purchasing these products. Novick Decl., Vol. XII, Ex. 103, pp. 17-25, ¶¶11-25, 27-30, 32-33.

RESPONSE: MF # 279 incorrectly assumes that Mr. Johnson's opinion and the FTC's "testing" make up undisputed facts. Mr. Johnson's opinion and the FTC's testing, which were contradicted by Mr. Ellis, are not established facts, but instead, simply opinions. *See* Response to MF # 259 above.

280. Daniel Sundin's sworn February 19, 2007 affidavit describes how 95% of IMI's sales are generated from software designed by IMI and sold through its websites. Sundin Affid., Vol. VIII, Ex. 89, p. 455, ¶12.

281. To illustrate "the steps that a member of the consuming public would follow to purchase one of these products" Sundin attaches to his February 19, 2007 affidavit screenshots of DriveCleaner, including a bogus scan advertisement used by the Defendants to market DriveCleaner. MF #61.

282. Sundin also attaches to his February 19, 2007 affidavit a "document generated by our Accounting Department based on IMI's internal sales records" that lists the Defendants' products, including WinFixer, WinAntiVirus, DriveCleaner, ErrorProtector, and SystemDoctor. Ex. E to Sundin Affid., Vol. VIII, Ex. 89, pp. 467 - 470.

283. Each of the statements in Sundin's February 19, 2007 affidavit are verified by Kristy Ross, who states in her own sworn affidavit dated March 6, 2007, that she has reviewed Sundin's affidavit and "is in agreement with [its] contents." Ross Aff., Vol. I, Ex. 2, p. 8.

RESPONSE: The assertion in MF #283 that Ms. Ross "verified" Daniel Sundin's affidavit, and by implication, swore to the accuracy of the assertions made therein is inaccurate. Ms. Ross' March 6, 2007 affidavit only states that she "read" the Jain and Sundin affidavits and was "in agreement with" their contents. (Ross Affidavit, ¶2.) Ms. Ross's statement is not a point-by-point verification of each of the paragraphs in these affidavits. Indeed, many of the paragraphs in the Jain and Sundin affidavits concern matters in which Ms. Ross was not involved, and of which she did not have personal knowledge and therefore would not have been able to testify to the statements made in Mr. Jain or Mr. Sundin's affidavits were she called as a witness in the Canadian litigation, or in this case.

284. Jettis Services Limited ("Jettis") was the payment processor for the defendants' operations from 2007 forward. D.E. #156 (Ex. 1), Moran Decl., p. 2.

285. Jettis processed more than $109 million in sales for the Defendants. MF #284.

286. Commencing with sales in late 2008, the Jettis database includes the name of the Defendants' software product the consumer purchased. D.E. #156 (Ex. 2), Novick Decl., Vol. XII, Ex. 103, p. 4, ¶9.

RESPONSE: MF #286 states that the Jettis database includes the names of "Defendants' software product the consumer purchased". There is no evidence that Ms. Ross participated in the creation or development of any software sold by IMI. The software for which the FTC contends she placed ads is set forth in D.E. #286-3, FTC Vol. XII, Ex. 103, pp. 28-30.

287. More than 130 products are included in this list, including several that both the FTC and defense experts agree use false and misleading system scans. Novick Decl., Vol. XII, Ex. 103, pp. 13-15, ¶4.

288. Many of the products included within the Jettis sales records were tested and found to be deceptive in the FTC's in-house testing. Novick Decl., Vol. XII, Ex. 103, pp. 17-25, ¶¶11-25, 27-30, 32-33.

289. 33 of the products included in the Jettis sales records are the subject of sworn consumer declarations submitted by the FTC, in which consumers detail the deceptive marketing and sales practices relied upon by the Defendants. Novick Decl., Vol. XII, Ex. 103, pp. 13-15, ¶4.

290. Both Kristy Ross and Marc D'Souza invoked the Fifth Amendment hundreds of times in this case in response to every substantive deposition question, interrogatory, and request for admission. Kristy Depo., Vol. VII, Ex. 65, pp. 1-73; D'Souza Depo., Vol. VII, Ex. 66, pp. 74-150.

RESPONSE: *See* Response to MF # 226.

291. Both Kristy Ross and Marc D'Souza were asked at deposition about the deceptive representations within IMI's software products. In response to this line of questions, both defendants invoked the Fifth Amendment over and over again. Ross Depo., Vol. VII, Ex. 65, pp. 1-73; D'Souza Depo., Vol. VII, Ex. 66, pp. 74-150.

RESPONSE: *See* Response to MF # 226.

292. In her March 6, 2007 affidavit to the Canadian Court, Ross admits that she worked for IMI from its inception in 2002 and that she was an original partner who formed IMI along with Sam Jain and Daniel Sundin. Ross Aff., Vol. I, Ex. 2, p.7, ¶1.

RESPONSE: MF #292 states that Ross admitted in her March 6, 2007 affidavit that she "worked for IMI from its inception in 2002 and that she was an original partner who formed IMI along with Sam Jain and Daniel Sundin." (Ross Affid., p. 7, ¶1.) This statement of a critical issue in this litigation is absolutely false. Ms. Ross' March 6, 2007 affidavit nowhere states that she was a "partner" or "original partner" at IMI. This fact is critical. Furthermore, although Ms.

Ross states that she worked at IMI since 2002, she nowhere states that she "formed IMI along with Sam Jain and Daniel Sundin." This fact too is critical.

293. Ross assumed the duties of Chief Operating Officer and Chief Technology Officer of IMI while Daniel Sundin battled an illness. Sundin Aff., Vol. VIII, Ex. 89, p. 456, ¶15.

RESPONSE: This statement is false. Sundin's affidavit nowhere states that Ms. Ross assumed any of his titles. What it states is that from "time to time" over the past 3 years Sundin suffered from an illness that did not permit him to devote as much time to his business endeavors as he would have liked and that some of his duties from time to time have been assumed by Ms. Ross.

294. Ross held the position of Vice President of Business Development for IMI beginning in 2006. Ross Aff., Vol. I, Ex. 2, p.7, ¶1.

295. Ross was identified as a Vice-President of IMI as late as June 21, 2008 in an email from Daniel Sundin to the Defendants' payment processor. D.E. #156 (Ex. 1), Moran Decl., p. 6.

RESPONSE: MF #295 states that Ms. Ross "was identified as a Vice President of IMI as late as June 21, 2008 in an email from Daniel Sundin to the Defendants' payment processor." The document nowhere states that the titles on the document ate with respect to IMI.

296. Ross routinely approved and requested payments for IMI's expenses, including advertising expenses for products such as WinAntiVirus, WinFixer, ErrorProtector, DriveCleaner, ErrorSafe, WinAntispyware, and SystemDoctor. Ex. I to D'Souza Affid., Vol. X, Ex. 97, pp. 224, 228, 230.

RESPONSE: The statement is misleading. Ms. Ross approved a number of entries for "affiliate payment swp." She requested advertising payments for the listed products which were approved by Marc D'Souza in 37 instances and Sam Jain in two instances. In only 2 instances did Ms. Ross herself approve advertising payments for the listed products.

297. Ross approved IMI payroll expenses, and the purchase of IMI computer equipment. Ex. I to D'Souza Affid., Vol. X, Ex. 97, pp. 245, 251.

RESPONSE: The reality is that Ms. Ross approved 5 entries on these pages which consist of 70-80 entries per page. The largest payroll expense she approved was $2,000 and the computer equipment was $9,300. Larger expenditures on these pages were approved by Marc D'Souza. Ex. I to D'Souza Affid., Vol. X, Ex. 97, pp. 245, 251.

298. From 2005-2007, Ross was one of only six individuals authorized to approve IMI's expenses. Ex. I to D'Souza Affid., Vol. X, Ex. 97, pp. 222-256.

RESPONSE: The reality is that Ms. Ross approved significantly fewer expenses then Marc D'Souza and the expenses she did approve were heavily weighted toward affiliate payments. Ex. I to D'Souza Affid., Vol. X, Ex. 97, pp. 222-256.

299. In several instances, Ross used a personal credit card to pay for IMI's advertising expenses and operating costs. MF #232; #pro, Vol. VII, Ex. 77, p. 372.

RESPONSE: MF #299 states that "Ross used a personal credit card to pay for IMI's advertising expenses and operating costs." While Ms. Ross paid for certain AdOn advertising expenses, these were the initial smaller costs paid at the time the accounts were set up. When the volume and the charges increased, credit cards of others including "MD" or Daniel Sundin were used to fund the ads. (Gieron Depo., RDX 1, pp. 171:17-25-172:1-17.) AdOn accounts were funded with credit cards of "MD" American Express card FTC 5, RDX 31, p. 1-9, 11-16, 18-29, 31, 33-39, 41-48, M D'Souza Visa FTC 5, RDX 31, p. 40, Daniel Sundin Visa FTC 5, RDX 31 p. 10, 17, 30 and Marc Cohen Visa FTC 5, RDX 31, p. 32. FTC 6, RDX 32, summarizes the credit cars for the MyGeek accounts which were in the names of "MD", Marc Cohen, M D'Douza (with his Carnegie Crescent address), and Daniel Sundin. Mr. Gieron testified at his deposition that it was common for employees to open accounts with MyGeek

under their own credit cards and then change to the credit card of a more senior member of the company when the charges increased, which is precisely what happened here. (Gieron Depo., RDX 1, pp. 171:17-25-172:1-17; 173:2-8.) The section of the chat log in which Ms. Ross' credit card is used to pay for "operating costs" was a unique emergency situation in which someone had failed to pay the bill for the Toronto servers such that the servers were going to be shut down. In that emergency situation, Ms. Ross was asked to step in and provide her card for payment and processing so that the Toronto servers would be switched back online. #pro, Vol. VIII, Ex. 77, p. 371-372 (note the FTC only cites to p. 372 but 371 is critical).

300. Ross was in charge of reorganizing IMI's operational structure. MF #10, Ex. C. to Sundin Affid., Vol. IX, Ex. 90, p. 58.

RESPONSE: The evidence cited does not support the assertion that Kristy Ross was in charge of reorganizing IMI's organizational structure. The email referred to as Ex. C to Sundin Affid., p. 58 is an email from Sam Jain to Marc D'Souza in which Ms. Ross is copied. The second page of this email mentions Kristy Ross only to state that "Broost and Kristy have been developing the operations plan and they can also offer valuable support in organizing the marketing plans." The Next line is "Once the basic strategy, org chart, and rough draft has been finalized; it can go out to matador, shiva, mike, and invisible, Conrad and other managers – and ask them to add and contribute their department plans to this." Rather than establish that Ms. Ross was an officer or owner or controlling person of IMI, as the FTC implies, this exchange suggests that Ms. Ross was an employee who was developing, with another employee, a suggested business plan to present to officers such as Jain and D'Souza.

301. Ross sent and received numerous emails regarding accounting issues, hiring, IMI's products, and key business decisions. Ross emails, Vol. VI, Ex. 60, pp. 229 - 261; Ross emails, Vol. VII, Ex. 72, pp. 283-284, 289 - 90, 292 - 294, 296-298, 301, 303-304, 306-07, 309, 311-12, 315, 317; Exs. M, N, V, BB to D'Souza Affid., Vol. X, Ex. 97, pp.

306-313; 351-354; Vol. 11, Ex. 97, pp. 4-5; D'Souza Affid., Vol. X, Ex. 97, p. 233-239.

RESPONSE: MF #301 refers to numerous emails and asserts that the emails concerned "accounting issues, hiring, IMI's products, and key business decisions". The FTC's characterization of these emails is not a fact but a point as to which there is significant factual dispute.

Emails at Vol. VI, Ex. 60, pp. 229-261 all involve Ms. Ross' accounts at AdOn.

Emails at Vol. VII, Ex. 72, pp. 283-284, 289-290, 292-294, 296-298, 301, 303-304, 306-307, 309, 311-312, 315 and 317 were emails about advertising links, the issue of domains expiring and needing renewal, the issue of email being down, issues with hosting services, generic products.

Emails at Exs. M, N, V. BB to D'Souza Affid., Vol. X, Ex. 97, pp 306-313; 351-354 concern requests to individuals in the Ukraine and James Reno for technical support, Emails from Sam Jain explaining and directing activity on which Ms. Ross and others are copied.

Vol. 11, Ex. 97, pp. 4-5 is likewise an email from Jain on which Ross and others are copied.

Vol. X, Ex. 97, p. 233-239 is an excerpt from the list of payment requests and approvals discussed at 297 and 298 above.

302. Ross sent an email to her co-defendants Reno and Jain, along with other IMI employees, discussing the launch of advertising for the rogue security product DriveCleaner. After referencing a webpage on the *drivecleaner.com* website, she states: This page is so incredibly slow, there is absolutely no way I can launch a campaign on this. There is absolutely no traffic currently going to drivecleaner project, so there is no way that can be the reason. Markb was saying there was major packet loss on this host the other day too, please check on this immediately. This is unacceptable and holding up the launch of the project. -Kristy. Ross email, Vol. VII, Ex. 72, p. 315.

RESPONSE: The FTC's characterization of DriveCleaner lacks support. There are two version of DriveCleaner at issue in this case, the free version and the paid version. Neither Kevin Johnson nor Scott Ellis tested the free version of DriveCleaner. (Expert Report of Kevin Johnson, RDX 33; Expert Supplemental Report of Kevin Johnson, RDX 34; Expert Report of Scott Ellis, RDX 7; and Supplemental Report of Scott Ellis, RDX 30.) Mr. Ellis tested the paid version of DriveCleaner and concluded as follows:

> DriveCleaner is a feature rich software that performs many of the same functions as comparable products, and does so successfully. DriveCleaner performs similarly to other system cleaners of the same time period and removed files as claimed. I detected no abnormal operation or suspicious behavior. DriveCleaner presented no issues or difficulties uninstalling from the test system at the completion of testing. Many major competitors including public companies such as Symantec and McAfee offer products with similar (and often less comprehensive) features than does DriveCleaner.

(Expert Report of Scott Ellis, RDX 7, p. 11.)

Mr. Ellis did not test the free version of DriveCleaner because he was not able to locate a free version of DriveCleaner in the materials he was provided by the FTC. (Supplemental Report of Scott Ellis., RDX 30, p. 2.) Nevertheless, at least in Mr. Ellis' expert opinion, DriveCleaner was a useful product comparable with other similar products available at the time and not a "rogue security product," as the FTC would have the Court believe.

> 303. Ross is asked to resolve problems from IMI employees whenever there were glitches with the production, launch, or maintenance of one of IMI's products. #mc, Vol. VII., Ex. 73, p. 326, 328, 329, 339, 340; # launch, Vol. VII, Ex. 74, p. 342-343, 351, 353-354.

RESPONSE: MF #303 asserts that "Ross is asked to resolve problems from IMI employees whenever there were glitches with the production, launch, or maintenance of one of IMI's products. The chat log excerpts cited fail to support this broad assertion.

#mc, Vol. VII., Ex. 73, p. 326 – *See* Response to MF #198 above Ex. 73, p. 328 – Ms. Ross' only role in the log is to ask Leo75 when some unknown task will be finished and she is told not today and maybe tomorrow. Ex. 73, p. 329 – This log concerns Ms. Ross being told that "karthik" is working on something for someone else and fuzzy has 500 things urgently that have not been done. Ex. 73, p. 339 – This log concerns corrections to creatives or ads given by Kristy Ex. 73, p. 340 – In this log there is a question as to whether shane got feedback from Kristy on elance ads. Elance is not a product at issue in the FTC Complaint. Ex. 74, p. 342 This log does not mention fuzzy or Kristy. Ex. 74, p. 343 – This log involves a decision as between "Leo75" and "Mike" that they should provide free opt in option in MAV free about which they assume they will have to discuss with Kristy. Fuzzy later discusses what appears to be her MyGeek ad campaign.

Ex. 74, 351 – This section of log fuzzy seems to approve creatives for Errorclean. The creatives reference errors blinking "when the scan completes" which contradicts notions of false scanning. Ex. 74, p. 353-354 – In this section of log, fuzzy gives an English language suggestion for a PrivacyTool ad and does not appear in p. 354. Not only is there no evidence for the claim that Ms. Ross is consulted "whenever" There are glitches for IMI products, these excerpts do not even establish that Ms. Ross had any kind of significant role in the categories alleged.

> 304. Ross approved the actual advertisements sent to third party ad networks for the Defendants' computer security products. # launch, Vol. VII, Ex. 74, p. 348, 346-47, 349-352.

RESPONSE: MF #304 states that "Ross approved the actual advertisements sent to third party ad networks for the Defendants' computer security products." These log sections do not support the assertion that Ms. Ross is approving ads but suggest that Ms. Ross is consulted on certain issues with certain ads particular with respect to English language usage and that she

weighs in on the topics. Moreover, while not mentioned by the FTC, p. 348 of Ex. 74 evidences Ms. Ross rejecting an ad as improper based on a representation she says is not permitted. Ex. 74, p. 346-47 – Fuzzy's only contribution to this exchange is to that that they had 30 creatives for Errorclen and they just needed to add aggression. Ex. 74, p. 348 – In this exchange, fuzzy rejects an ad as improper:

> <fuzzy> that ad – it says your current antivirus is not effective
> <fuzzy> can't say that

Also at p. 348 and into the next page of the log (not included by the FTC), fuzzy asks leo75 where a particular as for pcprivacytool is running. When Leo75 tells her "mostly USA", fuzzy logs; "we can't use that for RON that shows a nipple in it maybe dieter can run it, but we can't so let's get that ad redone without no nudity." Fuzzy continues, revising the idea of having dieter run the ad; "actually its best not to run it at all on ron that might upset people and give bad publicity." Ex. 74, p. 349, fuzzy logs that a particular French ad has to be changed because someone named vero says "it has misspellings, its sloppy errors all over the place. Fuzzy adds that "even that affiliate says its 'full of mistakes'". Contrary to the FTC assertion, fuzzy is not approving an ad but suggesting changes to an ad for the reasons she specifies. The page is also instructive as proof that ads were run through affiliates which was a source of difficulty in that it allowed others to control the content of certain ads. Ex. 74, p. 350, fuzzy asks leo75 about a "Sleepsea campaign". Leo75 here discusses having ads translated into "French, JP, Spanish" from which it does not even appear that whatever products are here being discussed are even being sold in the US. Fuzzy does state that for the marketing of whatever product they are discussing in these foreign countries that "aggression zero doesn't give sales" but fuzzy does not approve any ads. Ex. 74, p. 351, mike and leo75 are logging about "these creatives for Dieter GERS channel". Fuzzy reviews ads and with respect to a particular blinking functionality they

ask her about responds "yes its fine". However, leo75 again states "conv for Dieter GERS still 0.018-0.02 for mainstream." This exchange seems to be about ads being run in Germany. Additional evidence for the fact that these are non US ads is that at p. 348 when fuzzy discusses dieter, it is in the context of his being outside the US. Ex. 74, p. 352, there is a conversation about language problems with ads which appear to be French and Spanish. The conversation is about ads not working at all. Fuzzy does not approve anything.

305. In the Defendants' chat logs, Ross is observed making company decisions, demanding that employees fix problems and follow company procedures, and delegating IMI business projects. #mc, Vol. VII., Ex. 73, p. 322, 323, 330-31; #cio, Vol. VII, Ex. 85, 414-15; gigaispfuzzy, Vol. VII, Ex. 84, p. 413.

RESPONSE: MF #305 asserts that in the chat logs, "Ross is observed making company decisions, demanding that employees fix problems and follow company procedures, and delegating IMI business projects. The only assertion that these logs support is that fuzzy would become angry at certain IMI employees when they did not do the things they were supposed to do. Ex. 73, p. 322-3 – fuzzy complains that amaena landing pages should have been put into mediaplex and it was not done and expresses her displeasure with the department for not completing the task.

Ex. 73, p. 330-331 – Fuzzy asks for assistance with an ad

Ex. 85, p. 414 – Fuzzy asks about the status of fixing the host ecsecured in the Netherlands.

Ex. 85, p. 415 – Fuzzy admonishes kurbik about a situation in which she did not learn that domains were expiring until one day before expiration.

Ex. 84, p. 413 – fuzzy complains about dave and chris not doing what they are supposed to do. James Reno agrees and says that he can scream at them with text.

306. In one of the conversations from the Defendants' chat logs, Ross – using her alias fuzzy – threatens to fine an entire IMI department if they do not finish a project according to schedule: #mc, Vol. VII., Ex. 73, p. 323.

Jun 27 20:18:48 <fuzzy> it says it was taken at 12.24 today

Jun 27 20:18:50 <mike> is it done?
Jun 27 20:18:53 <fuzzy> its 8 hours later??
Jun 27 20:18:55 <fuzzy> how can it take 8 horus [*sic*]
Jun 27 20:19:42 <MihiR_OS> a bit delay from the dev side it ll finish asap
Jun 27 14:04:24 <MihiR_OS> yes dev ll finish it up today it self
Jun 27 14:04:30 <mike> ok 1 hr?
Jun 27 20:21:40 <fuzzy> please ensure its going to be done
Jun 27 20:21:44 <fuzzy> or im going to fine the department
Jun 27 20:21:53 <fuzzy> and MCs for not finishing it
Jun 27 20:22:05 <MihiR_OS> sure it ll finish

307. Defendant Ross began her relationship with MyGeek in 2004 using the IMI alias, Globedat. Gieron Depo., Vol. VIII, Ex. 87, p. 9 (31:4 - 31:14).

RESPONSE: MF #307 states that Ms. Ross used the "alias" globedat in her relationship with MyGeek. In MF #307, the FTC implies that Ms. Ross somehow tried to conceal her identity because she worked for globedat. Mr. Gieron did not state that Globedat was an alias, just that it was "an advertiser in our system." (Gieron Depo., RDX 1, p. 31:7-8.) There can be no doubt but that Ms. Ross gave complete and accurate contact information to MyGeek/AdOn. Kristy Ross was listed as the account holder at MyGeek. Account opening information listed her Seattle address which Mr. Gieron was familiar with as a place Kristy did reside. (Gieron Depo., RDX 1, pp. 168:5-22-169:1-4.) Kristy gave Gieron her contact phone number 206-730-2606. KR G4 p. 4 Gieron used this number to contact Kristy Ross. (Gieron depo., RDX 1, pp. 175:21-25-176:1-4.) Kristy opened numerous accounts at MyGeek under her own name Kristy Ross or KR. (FTC 4, RDX 35.) The FTC's suggestion that Ms. Ross was acting through an "alias," simply lacks merit and provides an unfair implication that Ms. Ross somehow acted inappropriately when the evidence is contrary.

308. Ross opened fifty-four (54) separate password-protected accounts between 2004-2006 and used virtually all of those accounts to disseminate ads for the Defendants' computer security products including WinFixer, DriveCleaner, WinAntivirus, WinAntispyware, FreeRepair, SystemDoctor, ErrorProtector, and ErrorSafe. MF # 11; Gieron Depo., Vol. VIII, Ex. 87, p. 11 (38:7 - 38:14).

RESPONSE: MF 308 states that Ms. Ross used MyGeek accounts to disseminate ads for a list of products in which they include "WinAntispyware". However, neither Mr. Gieron's deposition testimony nor that of the Declaration of FTC Investigator Novick supports the assertion. In fact, the FTC's own investigator's report suggests that Ms. Ross did not, in fact, place any ads for WinAntispyware. (D.E. #186-3, FTC Vol. XII, Ex. 103, pp. 28-30.)

309. Ross first used her own credit card to fund the MyGeek accounts, and then began using company credit cards in the names of her co-defendants, Marc D'Souza and Daniel Sundin. MF ## 11, 31, 232.

RESPONSE: The evidence supports that the credit cards of Ms. Ross and later Mr. Sundin and D'Souza were used but does that support that Ms. Ross was the one who used Sundin's and D'Souza's credit cards. To the contrary, the evidence was that anyone with the login and password information for a MyGeek account could access the accounts so it is not possible to know who actually did the funding of the accounts. Mr. Gieron testified:

> Q: And for each of those accounts, would Kristy Ross be able to set a different login and a different password if she wanted to?
> A: Yes
> Q: And would she be able to give those logins and those passwords to anyone within – any one of the other employees that worked at her company that she wanted to?
> A: Absolutely
> Q: And did AdOn have any policy against that or was that something that was common that people did?
> A: It's very common.
> (Gieron Depo., RDX, 1, pp. 165:23-25-166:1-8.)

310. Ross was the only person at IMI that dealt directly with MyGeek. MF # 213.

RESPONSE: *See* Response to MF ## 213 and 234 above.

311. When MyGeek had a problem with the ads placed by Ross, she was the one who responded; typically using the email address *kristy@globedat.com*. *See e.g.*, Ex. 23 to Gieron Depo., Vol. VIII, Ex. 87, p. 320.

312. Ross confirmed that her email address was *kristy@globedat.com* in the Defendants' company-wide chat logs. Network-fuzzy, Vol. VII, Ex. 76, p. 370.

313. Ms. Ross typically set her accounts at MyGeek to run the Defendants' ads over RON ("run of network"), meaning that the ads were not specifically targeted at users who were searching for something in particular, but rather the ads were placed on third party web sites indiscriminately throughout the Internet. *See, e.g.*, Gieron Depo., Vol. VIII, Ex. 87, p. 27 (101:6 - 101:18); 34 (131:9 - 132:1); Ex. 8 to Gieron Depo., Vol. VIII, Ex. 87, p. 192-197.

314. MyGeek routinely had to email Ross with requests that she submit new versions of her ads because the ads she submitted violated company policy by attempting to download software without consent ("forced downloads") or by spawning additional pop up windows. See e.g., Ex. 10 to Gieron Depo., Vol. VIII, Ex. 87, p. 206-226; Ex. 11 to Gieron Depo., Vol. VIII, Ex. 87, p. 227-235.

RESPONSE: MF #314 asserts that MyGeek had to "routinely email Ross with requests that she submit new versions of her ads because the ads she submitted violated company policy by attempting to download software without consent ("forced downloads") or by spawning additional pop up windows."

In support of this assertion the FTC cites FTC Exhibits 10 and 11 from the Gieron deposition. The first problem with this assertion is that in both FTC 10 and FTC 11 concern complaints about the appearance of ads at some point in time after Ms. Ross placed than rather than at the time she placed them. The distinction is critical because there is no evidence that Ms. Ross was to blame for the changes in her ads between the time she placed them and the time that they were complained about by MyGeek traffic partners. (Gieron Depo., RDX 1, pp. 5:19-20; 186:6-9; 186:10-25-187:1-23;193:11-25-194:1-4; 196:18-25-197:1-6; 229:1-12; 234:25-235:1-22; 266:1-6; 266:7-10; 266:11-16; 271:15-18; 277:21-25; 375:6-12.)

The second problem with this assertion is that the term "auto download" does not really mean a "forced download". Mr. Gieron testified that the ads discussed during his deposition did

not involve a true auto or forced download but rather ads which tries to get the user either advertently or inadvertently to click on a box to agree to an action. (Gieron Depo., RDX 1, pp. 217:17-25-218:1-25.) Significantly, Gieron also confirmed that neither of the ads in FTC 10 and 11 being complained about by MyGeek traffic partners were false. (Gieron Depo., RDX 1, pp. 245:5-11; 274:18-23.)

> 315. MyGeek tied a WinAntiVirus ad back to defendant Ross' accounts which contains a fake Microsoft Security Center window. The ad states, "Attention! Security Center has detected potential security vulnerabilities on your PC that may send private information and documents to a remote computer. One of the processes (win32res.exe) has just sent this information..." Ex. 18 to Gieron Depo., Vol. VIII, Ex. 87, p. 274.

RESPONSE: The first problem with the assertion is that there is only questionable and incomplete information that the particular ad in question was indeed traced back to Ms. Ross. Mr. Gieron stated that the account number and the Winantivirus domain are reasons why he would identify the ad being complained about to Ms. Ross. (Gieron Depo., RDX 1, pp. 295: 25-296:1-3, 12-14.) However, Gieron acknowledged that he could not establish that Ms. Ross came up with the ad and he does not have a link showing that Ms. Ross was the one who sent him the URL for the ad. (Gieron Depo., RDX 1, pp. 294:4-7, 295:3-7.) Furthermore, Gieron was unable to recall the structure of the ad pictured in FTC 18 and did not know if this is how the ad appeared that was approved or if this is how it appeared after complained about. (Gieron Depo., RDX 1, pp. 110:25-111:1-20.) Gieron testified; "I would say based on the context of the email, it would lean towards the WinAntivirus that was specific to Kristy's account. However, I don't have a URL to support that or the account designation." (Gieron Depo., RDX 1, pp. 113:6-11.) Second, Mr. Gieron acknowledged that the language of the ad was possibly accurate. (Gieron Depo., RDX 1, pp. 425:3-21.)

316. Whenever Ms. Ross was confronted by MyGeek with an ad that attempted to forcibly download software to consumers' computer or created excessive pop up windows, Ms. Ross would respond by providing new advertisements. See e.g. Ex. 12 to Gieron Depo., Vol. VIII, Ex. 87, p. 236-245.

RESPONSE: MF #316 asserts that "Whenever Ross was confronted by MyGeek with an ad that attempted to forcibly download software to consumers' computer or created excessive pop up windows, Ms. Ross would respond by providing new advertisements." The FTC cites Exhibit FTC 12 to the Gieron deposition in support of this assertion. Ex. 12 makes it clear that the issue that was being complained about was not "forcible" download but the "download prompt issue." (Gieron Depo., RDX 1, pp. 217:17-25-218:1-25.)

317. Ross was confronted by MyGeek with a WinFixer system scan advertisement that attempted to forcibly download software. The ad displays the oft-seen green scanning bar and "System Errors Found: 45." Ex. 15 to Gieron Depo., Vol. VIII, Ex. 87, p. 263-264.

RESPONSE: The first problem with the assertion in MF #317 is that the ad is not forcibly attempting to download software. Mr. Gieron testified that the ads discussed during his deposition did not involve a true auto or forced download but rather ads which tries to get the user either advertently or inadvertently to click on a box to agree to an action. (Gieron Depo., RDX 1, pp. 217:17-25-218:1-25.) In addition, despite the implication by the "oft seen green scanning bar" description, Mr. Gieron testified that based on the wording of the ad "Typical Quick System Scan", it is his assumption that the ad is not purporting to scan the computer. (Gieron Depo., RDX 1, p. 419: 17-21.)

318. Ross responded to the MyGeek complaint by saying: "Thanks for letting me know about this, I am in Europe, but will be back in the US for awhile as of Monday. ...I will try to send you some new link for this and hopefully it will resolve the problem." Ex. 15 to Gieron Depo., Vol. VIII, Ex. 87, p. 263.

RESPONSE: MF# 318 omits certain parts of Ms. Ross' email. The full quotation of Ms. Ross' response in FTC 15 is as follows: "Geoff, Thanks for letting me know about this. I am I Europe, but will be back in the US awhile as of Monday. *Sorry for not getting back to you sooner. I haven't heard of many issues lately as we were before*, but I will try to send you some new links for this and hopefully it will resolve the problem." (The portion omitted from the MF is in italics.)

319. The chat logs demonstrate that Ross routinely reviewed the content of the Defendants' deceptive ads, gave language suggestions, and approved the ads for distribution. #launch, Vol. VII, Ex. 74, p. 346-352.

RESPONSE: MF #319 states that "the chat logs demonstrate that Ross routinely reviewed the content of the Defendant's deceptive ads, gave language suggestions, and approved the ads for distribution." The logs cited do not support these assertions. MF #304 above contains a description of the content of each of the log pages cited by the FTC. In addition, the logs contain no support for the assertion that any ads discussed by Ms. Ross were deceptive.

320. In a conversation captured within the Defendants' chat logs, Ross reviews an ad for PCPrivacyTool. Ross states that the ad is too risque to run indiscriminately because – like the AdvancedCleaner fake scan ad displayed to the sixth grade student in Kansas discussed above – the ad features nude images. #launch, Vol. VII, Ex. 74, p. 348.

RESPONSE: MF #320 mischaracterizes the log at p. 348 of Ex. 74.

Ex. 74, p. 348 – In this exchange, fuzzy rejects an ad as improper:
<fuzzy> that ad – it says your current antivirus is not effective
<fuzzy> can't say that
Also at p. 348 and into the next page of the log (not included by the FTC), fuzzy asks leo75 where a particular as for pcprivacytool is running. When Leo75 tells her "mostly USA", fuzzy logs; "we can't use that for RON that shows a nipple in it maybe dieter can run it, but we can't so let's get that ad redone without no nudity." Fuzzy continues, revising the idea of having dieter run the ad; "actually its best not to run it at all on ron that might upset people and give bad

publicity." The reference to AdvancedCleaner ads and sixth grade students in Kansas is gratuitous and irrelevant as there is no evidence that Ms. Ross ever had any involvement in running AdvancedCleaner ads. Indeed, Gieron testified that the ad containing porn depicted in ¶24 of the FTC Complaint never ran at MyGeek/AdOn, that he had no recollection of globedat running any ads with porn, that he had no recollection of the ad shown on p. 9 of the FTC Complaint, and that he had no recollection of any ads for AdvancedCleaner running at MyGeek/AdOn. (Gieron Depo., RDX 1, pp. 442:8-25-443:1-3.) Moreover, the actual content of the log reveals that Ms. Ross is responsible for mandating that there not be nudity in ads that are run in the US.

> 321. In another conversation captured within the Defendants' chat logs, Ross was asked to approve a system scan advertisement and was asked whether the "system errors" and buttons should be highlighted. Ross states the ads looked fine and directed the employee to test them. #launch, Vol. VII, Ex. 74, p. 351.

RESPONSE: MF #321 characterizes the log at Ex. 74, p. 351. Ex. 74, p. 351 -- mike and leo75 are logging about "these creatives for Dieter GERS channel". Fuzzy reviews ads and with respect to a particular blinking functionality they ask her about responds "yes its fine". However, leo75 again states "conv for Dieter GERS still 0.018-0.02 for mainstream." This exchange seems to be about ads being run in Germany. Additional evidence for the fact that these are non US ads is that at p. 348 when fuzzy discusses dieter, it is in the context of his being outside the US.

> 322. In another conversation captured within the Defendants' chat logs, Ross is consulted about a new advertising campaign that will launch on the youth-oriented, social networking website MySpace. After being informed that the ads contain nudity, Ross orders that the ads be made even more aggressive, since "aggression zero doesnt [*sic*] give sales:" #launch, Vol. VII, Ex. 74, p. 350.
> May 21 08:41:19 <leo75> We have ready campaign for MySpace
> May 21 08:41:46 <leo75> dont know when they`ll start

May 21 08:41:46 <leo75> but now devs updating engine
May 21 08:41:46 <leo75> so need coordinate
May 21 08:41:53 <leo75> I mailed link for traffic to Sam
May 21 08:42:15 <fuzzy> what languages is it available for
May 21 08:42:17 <leo75> reg test results only few creatives doing good
May 21 08:42:30 <fuzzy> is it with aggression or without
May 21 08:42:48 <leo75> with nudity....we`ll fix it reg your conlusion
May 21 08:42:48 <leo75> agression totally zero now
May 21 08:43:01 <fuzzy> well we have to increase it
May 21 08:43:11 <fuzzy> aggression zero doesnt give sales [*sic*]

RESPONSE: MF #322 cites portions of the log at Ex. 74, p. 350. The log in this exhibit is from May 21, 2007. In one line quoted by the FTC, "Mike" logs "with nudity…we'll fix it re your conclusion." In the context of the log, fuzzy's "conclusion" for which they will "fix it" from May 14, 2007 of the chat log, pp. 228 and 229 of the chat log, FTC 025180-025181, RDX 36, is that it is not appropriate to run the ad with nudity on a ron campaign in the US. In addition, the comment about "aggression level zero" does not establish that the ads were deceptive. Mr. Gieron, at his deposition agreed that aggressive pop up ads were annoying but not false. (Gieron depo., RDX 1, p. 245:5-11; KRG 14, RDX 37.)

323. In another conversation captured within the Defendants' chat logs, Ross tells an IMI employee that the word "advertisement" had to come off of all the ads for all the Defendants' products. #launch, Vol. VII, Ex. 74, p. 352.

RESPONSE: MF #323 is false in stating that removing the French word "advertisement" applies to "all the Defendants' products". The date of the log is May 31, 2007. The references to products are "virusgarde" and "virusalarma" which from the language and context appear to be antivirus products marketed in France and in Spain which are not the subject of the FTC Complaint in this case. (FTC 025227-025228, RDX 38.)

324. Evidence from ValueClick establishes that Ross had her own password-protected account, which enabled her to upload the Defendants' advertisements onto the

ValueClick advertising system. Webster Depo., Vol. VI, Ex. 57, p. 63 (83:16 - 83: 24; 84:7 - 86:10); 69 (107:4 - 108:3); Ex. 13 to Webster Depo., Vol. VI, Ex. 57, p. 147.

RESPONSE: MF #324 states that evidence from Valueclick "establishes that Ross had her own password protected account which enabled her to upload the Defendants' advertisements onto the ValueClick advertising system." Mr. Webster testified at his deposition that the list of names on Ex. 13 from which the FTC draws the information for this fact was provided by the client, Revenue Response as part of a request to set up accounts. (Webster Depo., RDX 9, p. 106:4-7.) Mr. Webster did not know who at Revenue Response was responsible for compiling the list. (Webster Depo., RDX 9, p. 106:8-10.) He did not know if the email addresses on the list were real emails or if the individuals listed were real people. (Webster Depo., RDX 9, pp. 106:21-25-107:1.)

There is no evidence to support the assertion that Ms. Ross ever had a single dealing with the ValueClick network. There is no reference to Ms. Ross on documents containing billing information or billing contacts. (Webster Depo., RDX 9, p. 105:4-6.) Kristy Ross did not exchange any email correspondence with anyone at ValueClick. (Webster Depo., RDX 9, p. 105:17-23.) In fact Mr. Webster testified as follows:

> Q: With respect, Mr. Webster, to everything that you've looked at in preparation for your testimony in this case, all of the exhibits you've looked at and all the investigation that you've done in connection with your appearance at this deposition today, other than the one reference Mr. Arenson just drew your attention to, do you have any information to provide at all, any indication at all that an individual named Kristy Ross had a relationship with your network?
> A: I had not seen any other information to indicate that. Webster Depo., (108:7-18).

325. Ross' ValueClick account was created using Ross' alias "fuzzy" and the email address "kristy@globedat.com." Ex. 13 to Webster Depo., Vol. VI, Ex. 57, p. 147.

RESPONSE: *See* Response to MF # 324 above.

326. ValueClick's system retains the date of the most recent login, which in Ross's case, occurred on August 1, 2007. Ex. 13 to Webster Depo., Vol. VI, Ex. 57, p. 147.

RESPONSE: *See* Response to MF # 324 above.

327. Attached as Exhibit A to Jain's March 6, 2007 affidavit filed in the Canadian litigation, is a Profit & Loss ("P&L") Statement prepared by IMI's accounting department that reflects the income and expenses of IMI for years 2004, 2005, and 2006. Ex. A to Jain Aff., Vol. X, Ex. 96, p.14.

328. The P&L Statement shows that IMI grossed $74,638,578.76 from "Sales of Products and Services" between 2004 and the end of 2006. Once refunds and credit card chargebacks are subtracted, the net revenue for IMI is $71,614,133.18. Ex. A to Jain Aff., Vol. X, Ex. 96, p.14.

329. In the February 19, 2007 affidavit of IMI Chief Technology Officer Daniel Sundin, Sundin attaches as an exhibit "a document generated by [IMI's] Accounting Department based on IMI's internal sales records showing the growth in IMI's profits over the course of 2004 through 2006, as broken down by payment processor and website." Unlike the P&L Statement, the accounting submitted by Sundin categorizes revenues by product website. Ex. E to Sundin Affid., Vol. VIII, Ex. 89, pp. 467 - 470.

330. The FTC added together the sales totals for only those products in the IMI Accounting document attached to the Sundin Affidavit for which the FTC has corresponding consumer complaints alleging deceptive marketing, which resulted in total sales of $80,618,348.18. Novick Decl., Vol. XII, Ex. 103, p. 15, ¶15.

331. Jettis provided the FTC with multiple databases, which feature every credit card transaction processed by Jettis on the Defendants' behalf, along with, *inter alia*, the total price paid. D.E. #156 (Ex. 1), Moran Decl., p. 2, ¶1.

332. Nearly 16,000 of the records in the Jettis database also include the name of the actual product sold. D.E. #156 (Ex. 2), Novick Decl., p. 2-3, ¶6.

333. The Defendants' scareware revenues for 2007 - 2008 were $91,553,406.77. This figure does not include sales that were subject to a credit card chargeback or subsequently refunded. D.E. #156 (Ex. 2), Novick Decl., p. 4, ¶8.

RESPONSE: MF #333 refers to "Defendants' scareware revenues." There is no

evidence that defendant Ross received or collected or was allocated any revenue for her role as an IMI employee.

334. Consumer Cathy Mullen received pop up advertisements for AdvancedCleaner in March 2008. Mullen Decl., Vol. I, Ex. 32, p. 64.

335. The pop ups Mullen saw contained pornographic images and indicated that her computer was infected with viruses. As time went on, and the pop ups continued, the number of viruses detected in the ads increased and the pornographic pictures displayed in the ads became more explicit. Each time, the pop ups urged her to buy the AdvancedCleaner product. Mullen Decl., Vol. I, Ex. 32, p. 64, ¶¶2-3.

336. Mullen eventually had to cease using her computer because the AdvancedCleaner ads slowed her computer to a crawl. Mullen Decl., Vol. I, Ex. 32, p. 64, ¶5.

337. Mullen could not allow her grandchildren to use her computer out of fear that they would see the pornographic pictures in the incessant AdvancedCleaner ads. Mullen Decl., Vol. I, Ex. 32, p. 64, ¶5.

338. It took Mullen several months to get her computer repaired so that she could resume using it. Mullen Decl., Vol. I, Ex. 32, p. 64, ¶6.

339. Corey Keasling, a former system administrator, received a pop up advertisement for the Defendants' ErrorSafe product indicating that it had detected errors on his computer and urging him to click on the ad for a free scan of his computer. Keasling Decl., Vol. I, Ex. 23, p. 47-48, ¶¶2-3.

RESPONSE: MF #339 refers to "Defendants' ErrorSafe product". There is no evidence that Ms. Ross had any role in the creation or development of this product.

340. Because of his background, Keasling knew that it would be impossible for a pop up window to scan his computer and detect errors. Nonetheless, Keasling decided to click on the free scan ad in order to see what would happen. Keasling Decl., Vol. I, Ex. 23, p. 47-48, ¶¶3-4.

341. Once Keasling clicked on the advertisement he was taken to *errorsafe.com* where another scan occurred. Keasling Decl., Vol. I, Ex. 23, p. 47-48, ¶4.

342. The *errorsafe.com* scan displayed a number of Windows files it was purportedly scanning and then told him it detected a number of system errors. Keasling Decl., Vol. I, Ex. 23, p. 47-48, ¶4.

343. Keasling knew the ErrorSafe scan was a fraud because he was running the Linux operating system on his computer, and none of the Windows files the scan purportedly examined exist on his computer. Keasling Decl., Vol. I, Ex. 23, p. 47-48, ¶5.

344. In October 2008, Dan Fichana received a pop up warning message indicating that his computer was infected with viruses, and that his "Win32" file was infected. When he clicked on the warning message, he was taken to the VirusRemover2008 website where he was urged to buy the product to fix his computer. Fichana Decl., Vol. I, Ex. 11, pp. 24-25, ¶¶2-3.

345. Based on Fichana's extensive experience with computers, he was suspicious of the warning message and decided to test its accuracy. Fichana returned to the website where he first received the pop up warning using a computer running the Linux operating system, and received the exact same warning message telling him that the Win32 file was infected. Because the Win32 file does not exist on a computer running the Linux operating system, Fichana was able to conclude that the virus warning was a fraud. Fichana Decl., Vol. I, Ex. 11, pp. 24-25, ¶¶4-8.

RESPONSE: MF#345 is inaccurate to the extent that it attempts to imply that Ms. Ross had anything to do with VirusRemover2008. There is no evidence that Ms. Ross was associated with this product. In fact, as the FTC's own investigator, Mrs. Novak (nee Drexler), makes clear in her Declaration, Ms. Ross was not associated with VirusRemover2008. (*See* Drexler Dec, ¶ 110.; D.E # 186-3, Vol. XII, Ex. 103, Attachment A, pp. 28-30.)

346. The documents bates labeled FTC 15498-15741 and 048316-049021 are true and accurate copies of CRB's business records kept and maintained in the ordinary course of its business. CRB is a division of Royal Oak Financial. Shula Decl., Vol. VII, Ex. 71, pp. 279-281.

RESPONSE: The FTC has provided the Court and Ms. Ross with no foundation and no evidence with which to authenticate the referenced documents and so Ms. Ross's counsel has no way of determining from where these documents came or whether they are what they purport to

be.

347. The documents bates labeled FTC 074455-074496 are true and accurate copies of Tucows business records kept and maintained in the ordinary course of its business. Karkas Decl., Vol. VII, Ex. 68, p. 205.

RESPONSE: *See* Response to MF # 346.

348. The documents bates labeled FTC 013908-014379 are true and accurate copies of Junction Network's business records kept and maintained in the ordinary course of its business. Oeth Decl., Vol. VII, Ex. 55, p. 1.

RESPONSE: *See* Response to MF # 346.

349. The Canadian Affidavits and accompanying exhibits are true and accurate copies from the lawsuit *Innovative Marketing, Inc. v. D'Souza et. al.* filed in the Ontario Superior Court of Justice as copied, notarized, and authenticated by the United States Consulate General. Martins Decl., Vol. I, Ex. 1, pp. 1-3.

RESPONSE: *See* Response to MF # 346.

350. The documents bates labeled FTC 74252-74307 are true and accurate copies of Microsoft's business records kept and maintained in the ordinary course of its business. Declaration of Microsoft Trademark Paralegal Jennifer Bollen, Vol. VI, Ex. 59, pp. 170-171, ¶¶4-7.

RESPONSE: *See* Response to MF # 346.

351. The documents bates labeled FTC 049022, 071878-071882 are true and accurate copies of AdOn Network's business records kept and maintained in the ordinary course of its business. Ballapragada Decl., Vol. VIII, Ex. 88, pp. 441-42.

RESPONSE: *See* Response to MF # 346.

352. The encrypted hard drive that Dirk Kollberg sent to the Federal Trade Commission on or about September 30, 2009 is a fair and accurate copy of the Innovative Marketing Ukraine files he downloaded from the hard drive on his home computer. Kollberg Decl., Vol. VII, Ex. 69, pp. 248-52; Kollberg Depo., Vol. VII, Ex. 70, pp. 253-278.

RESPONSE: *See* Response to MF # 346. Responding further, starting in November 2008, Mr. Kollberg accessed internal servers that allegedly was once owned by IMI, but had been out of IMI's control for multiple years. (D.E. #186-3, Kollberg Decl., Vol. VII, Ex. 69, pp. 248-52, ¶ 3.; Kollberg Depo., RDX 39, p. 41.) Mr. Kollberg testified that he did not violate any anti-hacking laws because the server had been open to the public for some time and "[a]nyone who has a web browser could connect to the open servers. . . ." (D.E. #186-3, Kollberg Decl., Vol. VII, Ex. 69, pp. 248-52, ¶ 3.) Thus, any person with a computer could have gone onto this server before he copied it and changed any number of things. Mr. Kollberg testified at his deposition that accessing the internal IMI server which he pulled information was as easy as just entering the IP address and pressing return. (Kollberg Depo., RDX 39, pp. 58-59.) At this point, according to Kollberg, it was possible to access all of the information on the server. (Kollberg Depo., RDX 39, p. 59.) Mr. Kollberg also stated that a person would not need any specialized technical know-how or special software to access the server just as Mr. Kollberg did. (Kollberg Depo., RDX 39, pp. 101, 104, 153.) Mr. Kollberg further testified that from November 2008 through May 2009, he programmed his computer to crawl this server – which at that time was out of IMI's control and not owned by IMI – and download new files that it had not previously mirrored. (D.E. #186-3, Kollberg Decl., Vol. VII, Ex. 69, pp. 248-52, ¶ 4; Kollberg Depo., RDX 39, pp. 35-36.) Thus, the server was being changed and programs were being added during this period from November 2008 to May 2009, a time when IMI no longer controlled the server. Indeed, Mr. Kollberg testifies that during this time, contents from the server he was monitoring were being overwritten with the old version of the content being replaced by the newer content. (Kollberg Depo., RDX 39, p. 106.) Worse, it is not even possible to determine which of the server files were overwritten in the later time period because not all files even contained time

stamps. (Kollberg Depo., RDX 39, p. 107.)

This, it is impossible, therefore, to determine what information Mr. Kollberg gathered was from IMI and what was added by some other person or entity after IMI had terminated business and lost control of the server. Moreover, Mr. Kollberg also testified that he had an unnamed "friend" helping him gather this information and that this "friend," had downloaded information on to his own computer when Kollberg was not present. (D.E. #186-3, Kollberg Decl., Vol. VII, Ex. 69, pp. 248-52, ¶ 6.) Mr. Kollberg refused to identify this "friend" in his Declaration and he also refused to identify this "friend" at his deposition. D.E. #186-3, Kollberg Decl., Vol. VII, Ex. 69, pp. 248-52, ¶ 3; Kollberg Dep., RDX 39, p. 32.) Consequently, the Court and Ms. Ross's counsel are unable to test the trustworthiness of this nameless "friend" who assisted Mr. Kollberg in hisinternal server accessing activities. For all of these reasons, this information gathered by Mr. Kollberg and the undifferentiated part of this data gathered by some mystery person who apparently shall remain nameless, cannot be authenticated. Because of the inherent unreliability in the chain of custody for this information, it is impossible for anyone to say whether the referenced documents are "fair and accurate" copies of the information as it existed when IMI owned the server in question.

353. Ethan Arenson received an encrypted hard drive from Dirk Kollberg on or about October 2, 2009. Arenson Decl., Vol. XII, Ex. 101, p. 8, ¶3.

RESPONSE: *See* Response to MF # 346, 352.

354. Hugh Huettner received an encrypted hard drive from Ethan Arenson on or about October 25, 2009. Huettner Decl., Vol. XII, Ex. 102, p. 10, ¶10.

RESPONSE: *See* Response to MF # 346, 352.

355. Hugh Huettner created a forensic E01 image of the data named Winsoftware-0723137.005; copied it to a hard drive for storage; and placed a working copy on the

Storage Area Network (SAN). Huettner Decl., Vol. XII, Ex. 102, p. 10, ¶11.

RESPONSE: *See* Response to MF # 346, 352.

356. Huettner entered the forensic image into the evidence repository system for tracking and safe keeping. Huettner Decl., Vol. XII, Ex. 102, p. 10, ¶11.

RESPONSE: *See* Response to MF # 346, 352.

357. On or about October 28, 2009, Hugh Huettner received a hard drive from Ethan Arenson. Huettner Decl., Vol. XII, Ex. 102, p. 10, ¶12.

RESPONSE: *See* Response to MF # 346 352.

358. Hugh Huettner used approved forensic tools to make a forensic E01 image of the data on the First Reno hard drive. He then entered the forensic image into the evidence repository system for tracking and safe keeping. Huettner Decl., Vol. XII, Ex. 102, p. 11, ¶13.

RESPONSE: *See* Response to MF # 346, 352.

359. On or about October 14, 2010, Hugh Huettner received two hard drives from Ethan Arenson. Huettner Decl., Vol. XII, Ex. 102, p. 11, ¶14.

RESPONSE: *See* Response to MF # 346, 352.

360. Hugh Huettner copied the two hard drive images to the SAN to be used as working copies, and entered the drives into the evidence repository system for tracking and safe keeping. Huettner Decl., Vol. XII, Ex. 102, p. 11, ¶15.

RESPONSE: *See* Response to MF # 346, 352.

361. Documents bates labeled FTC 023819 - 024093, 024095 - 024159, 024161 - 024469, 046243 - 046268, 046270 - 046300, 049024 - 049037, as well as the electronic files produced the FTC by ValueClick and produced to the defense on a CD bates labeled FTC 023816 are true and accurate copies of ValueClick business records kept and maintained in the ordinary course of its business. Webster Depo., Vol. VI, Ex. 57, p. 45 (9:17 -12:25), p. 46 (13:1 - 15:14).

RESPONSE: *See* Response to MF # 346.

362. Documents bates labeled FTC 047336 – FTC 048315 as well as FTC Exhibits 3 - 26 to the Deposition of Geoff Gieron are true and accurate copies of AdOn Network business records kept and maintained in the ordinary course of its business. Gieron Depo., Vol. VIII, Ex. 87, p. 5 (15:9 - 15:25; 16:1 - 16:10).

363. Special Agent Eric Brelsford provided the FTC with a logical copy of electronic files seized during the execution of a search warrant at the business premises of ByteHosting Internet Services, LLC. Brelsford Decl., Vol. XII, Ex. 100, p. 3, ¶¶3, 5.

RESPONSE: *See* Response to MF # 346.

364. In October 2010, Special Agent Brelsford provided Ethan Arenson with copies of all of the forensic images seized during the search warrant described in MF # 364. Brelsford Decl., Vol. XII, Ex. 100, p. 4, ¶6.

RESPONSE: *See* Response to MF # 346. Shortly before the FTC submitted its summary judgment motion, the FTC provided the defense with a forensic copy of the electronic material taken from James Reno's Byte Hosting office during the execution of the FBI search warrant. The defense has not had an opportunity to analyze this data. However, the forensic copy alone does not provide adequate information for which to authenticate this electronic data. *See* Motion to Strike, filed contemporaneously herewith.

365. The documents bates labeled FTC 016253-016275 are true and accurate copies of Limelight Networks, Inc. business records kept and maintained in the ordinary course of its business. Torrez Decl., Vol. VI, Ex. 56, pp. 16-17.

RESPONSE: *See* Response to MF # 346.

Date: December 17, 2010

Respectfully submitted,

WINSTON & STRAWN LLP

/s/ *Carolyn P. Gurland*
Dan K. Webb, *pro hac vice*
Thomas L. Kirsch II, *pro hac vice*
Winston & Strawn LLP
35 West Wacker Drive
Chicago, Illinois 60601
(312) 558-5600
dwebb@winston.com
tkirsch@winston.com

Carolyn Gurland, *pro hac vice*
2731 North Mildred Avenue
Chicago, Illinois 60614
cgurland@comcast.net

Attorneys for Defendant Kristy Ross

CERTIFICATE OF SERVICE

I, Carolyn Gurland, hereby certify that in accordance with Fed. R. Civ. P. 5(a) a true and correct copy of the foregoing **Response to the FTC's Statement of Material Facts** was filed and served on all counsel of record via filing in the U.S. District Court for the District of Maryland Case Management/Electronic Case Filing (CM/ECF) system on December 17, 2010.

/s/ *Carolyn Gurland*